UNIVERSIDADE PRESBITERIANA MACKENZIE

Compreendendo a Disciplina de Gerenciamento de Riscos

RONALDO AFFONSO

São Paulo
2004

UNIVERSIDADE PRESBITERIANA MACKENZIE

Compreendendo a Disciplina de Gerenciamento de Riscos

Trabalho de apresentado a Universidade Presbiteriana Mackenzie, como requisito parcial para aprovação na matéria de Metodologia de Trabalho Científico.

Professor: Jacinto Mendes

RONALDO AFFONSO
CM: 30209935

São Paulo
2004

UNIVERSIDADE PRESBITERIANA MACKENZIE

Compreendendo a Disciplina de Gerenciamento de Riscos

Trabalho de apresentado a Universidade Presbiteriana Mackenzie, como requisito parcial para aprovação na matéria de Metodologia de Trabalho Científico.

Professor: Jacinto Mendes

Aprovada em Dezembro de 2004

BANCA EXAMINADORA

Professora Elida da Silva
Universidade Presbiteriana Mackenzie

Vivaldo Queiroz

Dedicatória

Gostaríamos de expressar nossa gratidão a toda nossa família e amigos na perseverança quanto ao apoio junto ao nosso trabalho , pois não seria possível realizar esse trabalho de tão grande importância para todo nosso grupo.

AGRADECIMENTOS

São muitos, os amigos que nos auxiliaram na realização desta trabalho, Muitos professores da Universidade Mackenzie, Unicamp, Puc, USP, Fatec foram de vital importância para que o objetivo deste trabalho sempre tivesse o mesmo escopo, aos nossos queridos amigos e potenciais profissionais conhecedores da área em que atuam, a agradecemos a Microsoft por ter cedido muitos textos que nos auxiliaram no nosso trabalho.

“Se você conhece você e seu inimigo ganhará todas as batalhas, mas se você conhece apenas você e não conhece seu inimigo, perderá algumas batalhas, e se você não se conhece e também não conhece o inimigo perderá todas as batalhas”

SUN TZU

Sumário

Resumo

Este módulo explica a práticas comprovadas derivadas de métodos de análise de segurança e processos formulados na MSF e na MOF. Ele detalhou os processos usados na SRMD para determinar os custos necessários para proteger os ativos da organização. Por fim, mostrou as etapas recomendadas para a formação de uma equipe de segurança para criar e executar planos de ação de segurança que impedirão ataques contra o ambiente da organização e permitirão que haja uma reação contra esses ataques.

Objetivos

Este módulo descreve uma metodologia comprovada para análise e gerenciamento de riscos. Ele se baseia na MSF (Microsoft Solutions Framework) e na MOF (Microsoft Operations Framework) para fornecer orientação e conselhos sobre como estabelecer uma diretiva de gerenciamento de segurança em sua organização. Identificando, categorizando e quantificando corretamente os riscos, você poderá agir da maneira mais apropriada e econômica para proteger o ambiente. Além disso, você poderá integrar o desenvolvimento da diretiva e do procedimento de segurança ao ciclo de vida de desenvolvimento da sua infra-estrutura de TI (Tecnologia da Informação).

Use este módulo para:

Identificar e quantificar os riscos do ambiente.

Identificar e quantificar o valor dos ativos de sua organização.

Usar esses valores quantificados para identificar as atividades mais adequadas e econômicas para proteger o ambiente.

Definir e gerenciar uma diretiva formal de gerenciamento de riscos de segurança.

Integrar o gerenciamento de riscos de segurança ao ciclo de vida da infra-estrutura de TI.

Definir processos para aprimorar a especialização em gerenciamento de riscos na sua organização por meio de iterações do ciclo do gerenciamento de riscos.

Aplica-se a

Este módulo se aplica aos seguintes produtos e tecnologias:

Toda a infra-estrutura de TI

Como usar este módulo

Use este módulo como orientação para o desenvolvimento e a integração de uma diretiva formal de gerenciamento de riscos de segurança que seja adequada para sua organização.

Para aproveitar este módulo ao máximo:

- Leia o módulo"**Definindo o cenário de segurança do Windows 2000**", antes do módulo atual. Ele apresenta a terminologia usada neste módulo e fornece uma visão geral das questões de segurança.
- Após ler o módulo atual, consulte os recursos listados na seção "Mais informações" no fim do módulo para obter mais orientações sobre questões específicas.

Introdução

Este módulo se baseia em práticas comprovadas de metodologias de análise de segurança em uso atualmente que aproveitam a MSF e a MOF. A MSF oferece orientações sobre as fases de planejamento, criação, estabilização e implantação do ciclo de vida do projeto nas áreas de arquitetura empresarial e implantação de infra-estrutura. A MOF fornece conselhos sobre como desenvolver ou aperfeiçoar sistemas de gerenciamento em operações de TI. Para obter mais detalhes sobre a MSF e a MOF, consulte a seção "Mais informações" no fim deste módulo.

O módulo define os três principais processos de orientação: a SRMD (Disciplina de Gerenciamento de Riscos de Segurança) e a Estrutura de Gerenciamento de

Riscos em termos das atividades de gerenciamento de riscos que ocorrem durante o ciclo de vida de um projeto de segurança.

Há três processos principais que uma organização pode usar para se tornar protegida e se manter protegida. As informações a seguir definem esses processos de uma forma geral.

1. Avaliação

   Esta fase envolve a coleta de informações relevantes sobre o ambiente da empresa a fim de se realizar uma avaliação da segurança. É preciso coletar dados suficientes para analisar com eficiência o estado atual do ambiente e, então, determinar o grau de proteção dos ativos em informações da organização contra possíveis ameaças. Além da avaliação da segurança, um Plano de Ação de Segurança será criado posteriormente para ser executado durante o processo de implementação.

2. Desenvolvimento e implementação

   Esta fase se concentra na execução de um Plano de Ação de Segurança a fim de implementar as alterações recomendadas no ambiente, que foram definidas na avaliação. Além do Plano de Ação de Segurança, é desenvolvido o Plano de Contingência de Riscos de Segurança.

3. Operação

   Esta fase envolve a realização de modificações e atualizações no ambiente, conforme o necessário para mantê-lo protegido. Teste de invasão e estratégias de resposta a incidentes são aplicados durante o processo operacional, o que ajuda a concretizar os objetivos de implementação de um projeto de segurança na organização. Também são realizadas atividades de auditoria e monitoramento dos processos operacionais a fim de manter a infra-estrutura intacta e protegida.

Práticas de gerenciamento de riscos de segurança e estrutura de segurança

Na execução do plano de segurança, dois tipos de atividades de gerenciamento de riscos são constantes durante o ciclo de vida do projeto. A primeira atividade é o gerenciamento de riscos inerentes ao próprio projeto. A segunda refere-se ao gerenciamento dos riscos associados aos componentes de segurança. Os riscos do projeto são avaliados somente durante o ciclo de vida do projeto, enquanto os riscos de segurança precisam ser avaliados durante todo o ciclo de vida da solução ou do sistema. A Risk Management Discipline da MSF serve como base para gerenciar os riscos das avaliações de projetos e de segurança. Exemplos prescritivos de gerenciamento de riscos de segurança serão descritos com mais detalhes no módulo "Aplicando a Disciplina de Gerenciamento de Riscos de Segurança" deste guia.

Neste guia de solução, é definida a SRMD, que se deriva da RMD (Risk Management Discipline) da MSF. Para distinguir claramente as duas atividades, a RMD é mencionada no contexto dos riscos do projeto, enquanto a SRMD refere-se à atividade de avaliação de riscos de segurança. A RMD é usada como principal ferramenta para o desenvolvimento da SRMD.

Os processos RMD e SRMD defendem uma abordagem proativa, avaliações contínuas de risco e a integração com o processo decisório ao longo do projeto e da operação do ambiente.

A segurança do sistema computacional deve ser feita de maneira proativa e contínua para garantir a segurança dos ativos em informações e para monitorar novas ameaças e vulnerabilidades. A segurança das informações deverá ser levada em consideração sempre que você adicionar novos recursos à infra-

estrutura de TI da sua organização. Além disso, talvez seja necessário alterar alguns processos e procedimentos comerciais para operar no ambiente modificado e oferecer a proteção a esses novos ativos em informações.

As nove etapas da Disciplina de Gerenciamento de Riscos de Segurança são:

Avaliação

1. Avaliação e atribuição de valores de ativos
2. Identificação de riscos de segurança
3. Análise e priorização dos riscos de segurança
4. Controle, planejamento e agendamento dos riscos de segurança

   Desenvolvimento e implementação

5. Desenvolvimento de correções de segurança
6. Teste de correções de segurança
7. Registro do conhecimento em segurança

   Operação

8. Reavaliação de ativos e riscos de segurança novos e alterados
9. Estabilização e implantação de contramedidas novas ou alteradas

Essas etapas estão incorporadas na SRMD como as três principais fases: avaliação, implementação e operação.

Avaliação

As seções a seguir incorporam tarefas de avaliação organizacional como base para o início de uma análise de segurança. A avaliação e a atribuição de valores de ativos são as primeiras etapas na análise de segurança, pois é necessário saber o que existe para avaliar a evolução dos riscos. O processo de análise de segurança é um conjunto de estratégias que permitem determinar que ativos devem ser protegidos no ambiente e a prioridade da proteção desses ativos.

Avaliação e atribuição de valores de ativos

A avaliação dos ativos refere-se ao valor das informações para as partes envolvidas e o esforço necessário para desenvolver essas informações. A atribuição de valores refere-se ao custo de manutenção de um ativo, a quanto custaria sua perda ou destruição e ao benefício que terceiros teriam ao obter

essas informações. O valor de um ativo deve refletir todos os custos identificáveis que poderiam resultar de um dano real ao ativo.

Identificação de riscos de segurança

A identificação de riscos de segurança permite que os membros da equipe do projeto discutam e façam emergir possíveis riscos de segurança. São coletadas informações sobre ameaças, vulnerabilidades, explorações e contramedidas.

Análise de riscos de segurança

A análise de riscos de segurança é usada para verificar possíveis ataques, ferramentas, métodos e técnicas que podem ser usados para explorar uma vulnerabilidade. A análise de riscos de segurança é um método de identificação de riscos e avaliação dos possíveis danos que podem ser causados, a fim de justificar as salvaguardas de segurança.

Uma análise de riscos de segurança tem três objetivos principais: identificar riscos, quantificar o impacto de possíveis ameaças e conseguir um equilíbrio financeiro entre o impacto do risco e o custo da contramedida. São coletadas informações para se estimar o nível de risco, de modo que a equipe possa tomar decisões fundamentadas sobre que riscos de segurança devem receber o maior esforço de correção.

Essa análise é, então, usada para priorizar os riscos de segurança e permitir que sua organização dedique recursos para atender às questões de segurança mais críticas.

Uma análise de riscos ajuda a integrar os objetivos do programa de segurança aos objetivos e requisitos de negócios da empresa. Quanto mais alinhados estiverem os objetivos de negócios e de segurança, mais bem-sucedida será a organização na concretização de ambos.

A análise também ajuda a empresa a delinear um orçamento adequado para um programa de segurança e os componentes de segurança que formam esse programa. Quando souber o valor dos ativos da empresa e entender as possíveis ameaças a que eles estão expostos, você poderá tomar decisões inteligentes sobre o quanto gastar na proteção desses ativos.

Controle, planejamento e agendamento dos riscos de segurança

O controle, o planejamento e o agendamento dos riscos de segurança usam as informações obtidas da análise de riscos de segurança para formular estratégias e planos de atenuação e contingência que os englobem. O agendamento dos riscos de segurança tenta definir um cronograma para as diversas estratégias de correção definidas durante a fase de criação de um projeto de segurança. Esse agendamento leva em consideração como os planos de segurança são aprovados e incorporados na arquitetura de informações, assim como os procedimentos de operações cotidianas padrão que devem ser implementados.

Desenvolvimento e implementação

O trabalho realizado durante o processo de avaliação permite que você desenvolva e implemente as contramedidas adequadas. Os resultados dos processos de avaliação permitem uma transição fácil para a implementação de estratégias eficientes de implantação de contramedidas e aprendizado de segurança.

Desenvolvimento de correções de riscos de segurança

O desenvolvimento de correções de riscos de segurança é o processo de usar os planos da fase de avaliação para criar uma nova estratégia de segurança que envolva gerenciamento de configurações, gerenciamento de patches, monitoramento e auditoria de sistemas, e diretivas e procedimentos operacionais. Como várias contramedidas estão sendo desenvolvidas, é importante garantir o controle e os relatórios precisos do progresso.

Teste de correções de riscos de segurança

O teste de correção de riscos de segurança ocorre após serem concluídos o desenvolvimento de estratégias de correção e as respectivas alterações no gerenciamento de sistemas, e após as diretivas e os procedimentos de determinação da eficiência serem escritos. O processo de teste permite que a equipe leve em consideração como essas alterações podem ser implantadas em um ambiente de produção. Durante o processo de teste, as contramedidas são avaliadas quanto à eficiência do controle dos riscos de segurança.

Aprendizado dos riscos de segurança

O aprendizado dos riscos de segurança formaliza o processo de registro de conhecimento sobre como a equipe protegeu os ativos e documenta as vulnerabilidades e explorações descobertas. À medida que o departamento de TI aprende novas informações de segurança, é preciso registrar e implantar mais uma vez essas informações para otimizar continuamente a eficiência das contramedidas que protegem os ativos da empresa. Além disso, a segurança precisa ser ensinada às comunidades da empresa por meio de treinamento ou boletins informativos de segurança.

Observação: essas etapas são uma orientação lógica e não precisam ser seguidas em seqüência para solucionar um determinado risco de segurança. As equipes de segurança passarão com freqüência pelas etapas de identificação, análise e planejamento à medida que ganharem experiência em questões de segurança, ameaças e vulnerabilidades de seus ativos em informações específicas.

Sua organização precisa determinar um processo de gerenciamento de riscos formal que defina como as contramedidas de segurança são iniciadas e avaliadas e sob que circunstâncias devem ocorrer transições entre as etapas para riscos de segurança individuais ou grupos de riscos.

Operação

Ciclos de operação sólidos e consistentes oferecem às equipes de segurança um mecanismo para obter resultados confiáveis e previsíveis. Executando o processo de avaliação no início do projeto de segurança, as equipes têm mais conhecimento de como reavaliar ativos novos e alterados em toda a empresa. A estabilização e a implantação de contramedidas novas ou alteradas para ativos novos e alterados tornam-se, então, parte da operação cotidiana da empresa.

Reavaliação de ativos e riscos de segurança novos e alterados

São essencialmente processos de gerenciamento de alterações, mas são também onde o gerenciamento de configurações de segurança é executado. Isso leva ao gerenciamento de versões quando as novas contramedidas e diretivas de segurança são concluídas.

Estabilização e implantação de contramedidas novas ou alteradas

Na fase de operação, esses processos são gerenciados por equipes de administração do sistema, da segurança e da rede. O monitoramento e o controle do serviço e o agendamento de tarefas são processos adicionais na fase de operação. Neles, os administradores de segurança aplicam contramedidas novas ou aprimoradas.

Central de atendimento de segurança, gerenciamento de incidentes e aprendizado de gerenciamento de problemas

Na fase de suporte, grupos operacionais na organização de TI oferecem suporte ao ambiente protegido por meio do gerenciamento preciso da central de atendimento de segurança e do gerenciamento controlado de incidentes e da escalação de problemas.

Gerenciamento financeiro, de nível de serviço e de disponibilidade

A MSF e a MOF são práticas comprovadas, projetadas para ajudá-lo a desenvolver, implantar e manter um programa de gerenciamento de segurança preciso. O uso adequado dessas práticas permite a criação de um ambiente que ofereça integridade, confidencialidade e disponibilidade de recursos.

O gerenciamento de segurança é otimizado pelo rigor no gerenciamento de nível de serviço, gerenciamento financeiro, gerenciamento da comunidade de serviços, gerenciamento de disponibilidade, gerenciamento de capacidade e gerenciamento de força de trabalho.

_

Estrutura de gerenciamento de riscos de segurança

Visão geral

A estrutura aproveita o modelo de processo da MSF e descreve uma seqüência geral de atividades para criar e implantar soluções de segurança de TI. Em vez de prescrever uma série específica de procedimentos, a estrutura é flexível o suficiente para acomodar uma ampla gama de processos de TI. O modelo de processo aborda o ciclo de vida de uma solução, desde o começo do projeto até a implantação ativa.

Figura 1

Etapas do modelo de processo da estrutura de segurança por fase

O modelo de processo da MSF pode ser usado para desenvolver aplicativos e implantar tecnologia de infra-estrutura. Ele segue um ciclo iterativo projetado para acomodar alterações de requisitos do projeto por meio de ciclos curtos de desenvolvimento e versões incrementais da solução. O gerenciamento de riscos e os ciclos de teste contínuos tornam isso possível.

Diversas perguntas importantes sobre o projeto são feitas e respondidas ou discutidas em cada etapa do modelo de processo, como: A equipe concorda com o escopo do projeto? A equipe planejou o suficiente para prosseguir? A equipe criou o que disse que iria criar? A solução está funcionando adequadamente para os clientes e parceiros da organização? Estes seis processos principais de um projeto de segurança associados à figura acima são discutidos resumidamente aqui.

1. Início da definição do projeto
   A fase inicial do projeto atende a uma das necessidades mais fundamentais para o sucesso do projeto de segurança: unificar a equipe do projeto e o programa de segurança. O processo de início da equipe continua até o refinamento, no fim da fase inicial. Todos os membros da equipe têm uma

visão clara do que desejam conseguir com uma solução de segurança e das necessidades da empresa em relação à segurança. Essa fase se concentra na identificação do problema ou da oportunidade da empresa ou no gerenciamento de segurança. Todas as partes envolvidas no gerenciamento de segurança precisam definir objetivos, suposições e restrições durante esses processos.

2. Avaliação e análises de segurança
A avaliação e as análises do gerenciamento de segurança são processos que ocorrem na fase de planejamento da metodologia da MSF. Esses processos incluem avaliação da organização, atribuição de valores de ativos, identificação de ameaças, avaliação de vulnerabilidades e avaliação de riscos de segurança. Juntos, eles formam o planejamento envolvido em uma implantação bem-sucedida de contramedidas.
3. Desenvolvimento de correções de segurança
Informações obtidas nas fases de avaliação e de análise de segurança criam um meio para o desenvolvimento de correções de segurança. Durante esses processos, os desenvolvedores trabalham constantemente no desenvolvimento, teste e validação de contramedidas para remediar os riscos identificados nas fases anteriores do projeto. Esses processos de desenvolvimento de correções de segurança são testados pela equipe de desenvolvimento e avaliados segundo critérios de qualidade.
4. Teste de correções de segurança e teste de funcionalidade de recursos
Os processos de teste de correções de segurança e de teste de funcionalidade de recursos têm resultados menos previsíveis. Resultados imprevistos do teste funcional são identificados e gerenciados durante a fase de estabilização pelos processos de teste. Apesar de a fase de criação se basear em planos e especificações conhecidos, o número e a gravidade dos erros que serão encontrados são sempre desconhecidos. As técnicas de convergência de erros e resposta sem erros são usadas pela Microsoft para medir a qualidade da solução e prever a data de lançamento durante essa fase.
5. Implantação de contramedidas e diretivas de segurança

Os processos de implantação de contramedida e de diretiva de segurança continuam ao longo da fase de implantação da metodologia MSF e no ciclo de processo MOF. Esse processo de implantação de contramedidas organiza os tipos de contramedidas e diretivas de segurança em dois tipos, principal e de site, e seus respectivos componentes de segurança. Componentes de segurança específicos encontram-se em um local central ou principal que envolve toda a solução de segurança. Componentes específicos de sites encontram-se em locais individuais que permitem aos usuários acessar e usar a solução de segurança.

6. Conclusão da implantação
   O conhecimento do gerenciamento de riscos de segurança é um processo registrado próximo à etapa de conclusão da implantação. O registro das lições aprendidas próximo à implantação coloca a solução em um estado operacional e entregam o projeto concluído ao ciclo de processo da MOF.

Para obter mais detalhes sobre os processos do projeto de segurança, consulte o guia *Microsoft Solution for Security Services*.

Criando a equipe do programa de segurança

Durante o processo de avaliação do modelo de processo da MSF, ocorre uma etapa fundamental para a proteção do ambiente, que é a criação de um programa de segurança. O fundamento desse programa de segurança é determinar objetivos, escopo, diretivas, prioridades, padrões e estratégias para a segurança total da organização. Os membros do programa de segurança são executivos seniores da empresa. O grupo de administração de segurança é, portanto, composto de gerentes de nível médio e de suas equipes que implementam e gerenciam as diretivas determinadas pelo programa de segurança.

Um programa de segurança deve ser desenvolvido com uma abordagem de cima para baixo, o que significa que o início, o suporte e a direção devem vir da gerência superior, sendo aplicados pela gerência média e, finalmente, incluir os membros da equipe. O suporte, no entanto, pode ser uma combinação de desenvolvimento e defesa de idéias que partam do nível superior, do nível inferior ou do nível médio no gerenciamento de segurança. Hoje, diversas

empresas usam uma abordagem de baixo para cima para o desenvolvimento e o suporte, em que o departamento de TI desenvolve um plano de segurança sem suporte e direção adequados da gerência. Isso pode fazer com que o programa de segurança fique desalinhado com os objetivos comerciais mais amplos da organização.

A gerência sênior deve começar a criar o programa de segurança atribuindo funções e responsabilidades dentro da organização, que sejam necessárias para um início bem-sucedido. O envolvimento da gerência sênior mantém a eficiência e a evolução do programa à medida que os ambientes comercial e técnico mudam. A criação de funções em um programa de segurança confirma que a organização reconhece a segurança como parte integrante de seu negócio, em vez de apenas uma preocupação.

Além de um programa de segurança, a gerência deve estabelecer um grupo de administração de segurança. Esse grupo é diretamente responsável pelo monitoramento da maior parte das facetas de um programa de segurança. Geralmente, o programa de segurança em uma organização desenvolve diretivas de segurança, enquanto o grupo de administração de segurança impõe e monitora configurações de segurança.

Dependendo da organização, de suas necessidades de segurança e do tamanho do ambiente, a administração de segurança pode consistir em uma pessoa ou um grupo de indivíduos que trabalham de maneira centralizada ou descentralizada.

Avaliação

A estrutura de segurança para avaliação de ameaças, descrita no modelo de processo, é projetada para ajudar os profissionais de segurança a desenvolver uma estratégia para proteger a disponibilidade, a integridade e a confidencialidade de dados na infra-estrutura de TI de uma organização. Pode ser de interesse dos gerentes de recursos de informação, dos diretores de segurança de computadores e dos administradores, e especialmente valiosa para os que tentam estabelecer diretivas de segurança de computadores. A estrutura oferece uma abordagem sistemática dessa importante tarefa e, como precaução final, também envolve a definição de planos de contingência em caso de desastre.

Confidencialidade

A infra-estrutura de TI da organização pode conter informações que exigem proteção contra divulgação não autorizada. Os exemplos incluem a disseminação de informações com data programada, como relatórios de resultados, informações pessoais ou informações comerciais proprietárias. A confidencialidade garante que a capacidade de fornecer o nível necessário de segredo seja imposta em cada junção do processamento de dados e impede a divulgação não autorizada. Um nível consistente de confidencialidade deve ser mantido enquanto os dados residem em sistemas e dispositivos na rede, quando são transmitidos e quando atingem o destino.

Integridade

A infra-estrutura de TI contém informações que devem ser protegidas contra modificação não autorizada, não prevista e não intencional. Os exemplos incluem informações censitárias, indicadores econômicos ou sistemas de transações financeiras. A integridade é mantida quando a precisão e a confiabilidade das informações e dos sistemas são garantidas e a modificação não autorizada dos dados não é possível.

Disponibilidade

A infra-estrutura de TI contém informações ou fornece serviços que devem estar disponíveis de maneira apropriada para atender aos requisitos da missão ou evitar perdas substanciais. Os exemplos incluem sistemas fundamentais para segurança, suporte a vida e conectividade de rede consistente. A disponibilidade garante confiabilidade e acesso apropriado a dados e recursos para indivíduos autorizados.

Os administradores de segurança precisam decidir quanto tempo, dinheiro e esforço deve ser gasto para desenvolver as diretivas e os controles de segurança adequados. A organização deve analisar suas necessidades específicas e, então, determinar seus recursos, requisitos de cronograma e restrições. Sistemas de computador, ambientes e diretivas organizacionais são diferentes, dificultando a estratégia para proteger grupos de computadores na organização.

Apesar de a estratégia de segurança poder economizar um tempo valioso da organização e fornecer lembretes importantes do que precisa ser feito, a

segurança não é uma atividade realizada uma única vez. Ela é parte integral do ciclo de vida do sistema para o ambiente. As atividades descritas neste módulo geralmente exigem atualização periódica ou revisão adequada. Tais alterações são feitas quando as configurações ou outras condições mudam de forma significativa ou quando regulamentos e diretivas organizacionais exigem mudanças. É um processo iterativo que nunca termina e deve ser revisado e testado periodicamente.

Avaliação organizacional

O estabelecimento de um conjunto eficiente de diretivas e controles de segurança exige o uso de uma estratégia para determinar as vulnerabilidades que existem nos sistemas de computador e nas diretivas e controles de segurança atuais que os protegem. Sua revisão deve registrar áreas do ambiente em que faltam diretivas, assim como examinar documentos de diretivas existentes. Além das revisões de diretivas, a equipe jurídica da organização deve garantir que todas as diretivas de segurança estejam em conformidade com a diretiva jurídica da empresa. O status atual das diretivas de segurança de computadores pode ser determinado revendo-se a seguinte lista:

- Diretivas de segurança física de computadores, como controles de acesso físico

- Diretivas de segurança de dados (controle de acesso e controles de integridade)

- Planos e testes de contingência e recuperação de desastres

- Reconhecimento e treinamento de segurança de computadores

- Diretivas de gerenciamento e coordenação de segurança de computadores

Outros documentos de diretivas que contenham informações confidenciais, incluindo:

- Senhas de BIOS de computador

- Senhas de configuração de roteador
- Documentos de controle de acesso
- Outras senhas de gerenciamento de dispositivos

Análise de ameaças

A criação de listas de ameaças (a maioria das organizações pode identificar várias) ajuda o administrador de segurança a identificar as diversas explorações que podem ser usadas em um ataque. É importante que os administradores sempre atualizem seus conhecimentos nessa área, pois novos métodos, ferramentas e técnicas para burlar as medidas de segurança estão sempre sendo inventados.

O processo de análise de ameaças é descrito na fase de planejamento da figura 1 para determinar os ataques que podem ser esperados e, assim, desenvolver formas de defesa contra esses ataques. É impossível se preparar contra todos os ataques; assim, prepare-se para os ataques mais prováveis que a organização possa esperar. É sempre melhor impedir ou minimizar os ataques do que corrigir os danos causados por eles.

Para minimizar os ataques, é necessário compreender as diversas ameaças que causam riscos aos sistemas, as técnicas correspondentes que podem ser usadas para comprometer os controles de segurança e as vulnerabilidades que existem nas diretivas de segurança. A compreensão desses três elementos de ataques ajuda a prever sua ocorrência, e até mesmo o momento ou o local. Prever um ataque é o mesmo que prever sua probabilidade, o que depende da compreensão de seus diversos aspectos. Esses aspectos podem ser expressos na seguinte equação:

Motivos da ameaça + Métodos de exploração + Vulnerabilidades dos ativos = Ataque

Um atacante mal-intencionado pode usar diferentes métodos para iniciar o mesmo ataque. Assim, a estratégia de segurança deve ser personalizada para cada método que cada tipo de agente de ameaça pode explorar.

Avaliação de vulnerabilidades

A avaliação das necessidades de segurança da organização deve incluir a determinação de suas vulnerabilidades em relação a ameaças conhecidas. Essa avaliação envolve reconhecer os tipos de ativos que a organização tem e que tipo de dano eles podem sofrer.

Determinando os danos possíveis de um ataque

Os danos possíveis aos ativos no ambiente podem variar de pequenas falhas de computador até perdas de dados catastróficas. Os danos causados ao sistema dependerão do tipo de ataque. Se possível, use um ambiente de teste ou de laboratório para esclarecer os danos resultantes de diferentes tipos de ataques. Isso permitirá que a equipe de segurança avalie com precisão os danos físicos. Nem todos os ataques causam o mesmo tipo ou a mesma quantidade de danos. Os testes que podem ser executados incluem:

- Uma simulação de ataque de vírus de email em um sistema de laboratório, seguida de uma análise para determinar os danos causados e os possíveis procedimentos de recuperação necessários.
- Um teste para determinar se os funcionários estão sujeitos a ataques de engenharia social, que tentam conseguir o nome de usuário e a senha de um funcionário desavisado.
- Uma simulação de desastre em um centro de dados. Medir o tempo de produção perdido e o tempo até a recuperação.
- Uma simulação de um ataque de vírus mal-intencionado. Medir o tempo necessário para recuperar um computador. Esse fator de tempo pode ser multiplicado pelo número de computadores infectados no sistema para avaliar a quantidade de tempo de inatividade ou a perda de produtividade.

Também é aconselhável envolver uma equipe de resposta a incidentes no processo, pois é mais provável que ela, e não um único indivíduo, observe todos os diferentes tipos de danos que ocorreram. Uma equipe de respostas a

incidentes gerencia a priorização de incidentes de segurança e os caminhos de escalação para resolvê-los.

Determinando as vulnerabilidades ou os pontos fracos que um ataque pode explorar

Se as vulnerabilidades que um ataque específico explora puderem ser descobertas, será possível alterar ou criar diretivas e controles de segurança para minimizar as vulnerabilidades. A determinação do tipo de ataque, ameaça e método facilita a descoberta de vulnerabilidades existentes. Isso pode ser comprovado com um teste de invasão.

Planejamento e agendamento de riscos de segurança

Para cada método de exploração, o plano de segurança da organização deve incluir estratégias proativas e reativas.

A estratégia proativa, ou pré-ataque, é um conjunto de etapas que ajudam a minimizar as vulnerabilidades da diretiva de segurança existente e a desenvolver planos de contingência. A determinação dos danos que um ataque causará em um sistema e dos pontos fracos e das vulnerabilidades exploradas durante o ataque ajuda no desenvolvimento de uma estratégia proativa.

A estratégia reativa, ou pós-ataque, ajuda a equipe de segurança a avaliar os danos causados pelo ataque, corrigir os danos ou implementar o plano de contingência desenvolvido na estratégia proativa, documentar e aprender com a experiência e reabilitar as funções de negócios assim que possível.

Estratégia proativa

A estratégia proativa é um conjunto de etapas predefinidas que devem ser seguidas para impedir ataques antes que eles ocorram. Essas etapas incluem verificar como um ataque poderia afetar ou danificar o sistema de computador e as vulnerabilidades que ele explora (etapas 1 e 2). O conhecimento obtido nessas avaliações pode ajudar a implementar diretivas de segurança que vão controlar ou minimizar os ataques. Estas são as quatro etapas da estratégia proativa:

1. Determinar os danos que o ataque causará.
2. Determinar as vulnerabilidades e os pontos fracos que o ataque vai explorar.
3. Minimizar as vulnerabilidades e os pontos fracos relacionados ao ataque

específico indicado nas duas primeiras etapas.

4. Determinar o nível apropriado de contramedidas a serem implementadas.

Seguir essas etapas para analisar cada tipo de ataque resultará em um benefício indireto: começará a surgir um padrão dos fatores comuns a diferentes ataques. Esse padrão pode ser útil para determinar as áreas de vulnerabilidade que representam o maior risco para a empresa.

Observação: também é necessário equilibrar o custo da perda de dados e o custo da implementação dos controles de segurança. Ponderar esses riscos e custos faz parte de uma análise de riscos do sistema.

Estratégia reativa

Uma estratégia reativa é implementada quando a estratégia proativa para o ataque falha. A estratégia reativa define as etapas que devem ser seguidas durante ou após um ataque. Ela ajuda a identificar os danos causados e as vulnerabilidades que foram exploradas no ataque. Uma estratégia reativa também determina por que um ataque ocorreu, como corrigir os danos causados e como implementar um plano de contingência.

As estratégias reativas e proativas trabalham juntas para o desenvolvimento de diretivas e controles de segurança no sentido de minimizar ataques e seus danos. A equipe de resposta a incidentes deve ser incluída nas etapas seguidas durante ou após o ataque a fim de ajudar a avaliar, documentar e aprender com o evento.

As três etapas a seguir estão envolvidas na estratégia reativa:

1. Limitar os danos.

   Conter os danos causados durante o ataque permite limitar a extensão dos danos. Por exemplo, se houver um vírus no ambiente, você tentará liminar os danos assim que possível desconectando os servidores da rede, mesmo antes de descobrir quantos servidores podem ter sido afetados. Isso deve ser feito o mais rapidamente possível.

2. Avaliar os danos.

   Determinar os danos causados durante o ataque. Isso deve ser feito com rapidez para que as operações da organização sejam reiniciadas assim que possível. Se não for possível avaliar os danos de maneira adequada, um plano de contingência deverá ser implementado para que as operações de

negócios normais e a produtividade possam continuar.

3. Determinar a causa dos danos.
   Para determinar a causa dos danos, é necessário compreender que recursos o ataque visava e que vulnerabilidades foram exploradas para obter acesso ou interromper os serviços. Revise os logs do sistema, os logs de auditoria e as faixas de auditoria. Geralmente, essas revisões ajudam a descobrir a origem do ataque no sistema e os recursos que foram afetados.
4. Corrigir os danos.
   É muito importante que os danos sejam corrigidos o mais rapidamente possível a fim de restaurar as operações de negócios normais e os dados que tenham sido perdidos durante o ataque. Os planos e procedimentos de recuperação de desastres da organização devem abranger a estratégia de restauração. A equipe de resposta a incidentes também deve estar disponível para lidar com o processo de restauração e recuperação e para fornecer orientações sobre o processo de recuperação. Durante esse processo, os procedimentos de contingência são realizados para isolar e limitar a disseminação dos danos.

Plano de contingência

O plano de contingência é alternativo e foi desenvolvido caso um ataque entre no sistema e danifique dados ou outros ativos, resultando em interrupção das operações normais da empresa ou em redução da produtividade. O plano de contingência será seguido se o sistema não puder ser restaurado de maneira adequada. Em última instância, o objetivo é manter a disponibilidade, a integridade e a confidencialidade dos dados; é o equivalente a um "plano B".

Planos de contingência devem ser criados para responder a cada tipo de ataque ou ameaça. Cada plano deve conter um conjunto de etapas a serem seguidas caso haja um ataque. Eles devem:

- Indicar quem faz o que, quando e onde para manter a organização funcionando.
- Ser ensaiados periodicamente para manter a equipe atualizada com as etapas de contingência mais recentes.
- Abranger a restauração de informações de servidores de backup.

- Englobar a atualização de software antivírus, service packs e hotfixes.
- Abordar os procedimentos de mudança dos servidores de produção para outro local. Se houver orçamento, as replicações dos servidores de produção devem ser reunidas em locais de contingência estratégicos.
- Incluir uma revisão de fechamento das diretivas de segurança e dos planos de contingência atuais.

Os pontos a seguir descrevem as diversas tarefas de avaliação que devem ser realizadas ao se desenvolver o plano de contingência:

- Avaliar as diretivas e os controles de segurança da organização para aproveitar todas as oportunidades que minimizem as vulnerabilidades. A avaliação deve envolver o plano e os procedimentos de emergência atuais da organização, assim como sua integração ao plano de contingência.
- Avaliar os procedimentos de respostas de emergência atuais e seus efeitos nas operações da empresa.
- Desenvolver respostas planejadas para ataques e integrá-las aos planos de contingência, observando até que ponto elas são adequadas para limitar os danos e minimizar o impacto de um ataque nas operações de processamento de dados.
- Avaliar procedimentos de backup, incluindo as documentações e os testes de recuperação de desastres mais recentes, a fim de medir sua adequação e incluir os resultados das avaliações nos planos de contingência.
- Avaliar os planos de recuperação de desastres a fim de determinar se as etapas envolvidas são adequadas para fornecer um ambiente operacional temporário ou de longo prazo. Os planos de recuperação de desastres devem incluir o teste dos níveis de segurança exigidos pela organização para que a equipe de segurança possa determinar se pode continuar a impor a segurança durante todo o processo de recuperação, operações temporárias e retorno ao local de processamento original da organização ou mudança para um novo local.
- Criar um documento detalhado descrevendo as descobertas necessárias para

seguir as etapas mencionadas acima. Este documento deve listar:

- Detalhes sobre cenários de usuários para testar os planos de contingência.

- Detalhes sobre o impacto que dependências, como obter ajuda externa e recursos essenciais, terão nos planos de contingência.

- Uma lista de prioridades observadas nas operações de recuperação e a lógica usada para estabelecê-las.

- Detalhes sobre caminhos de escalação para que, quando um plano de contingência for executado, todos os problemas que possam surgir dele sejam escalados com clareza para a equipe mais eficiente de TI ou de operações da empresa.

Implementação

Cuidado para não implementar controles que sejam muito restritivos, pois a disponibilidade das informações poderá se tornar um problema. Deve haver um equilíbrio cuidadoso entre os controles de segurança e o acesso às informações.

Teste de simulação de ataque

O último elemento de uma estratégia de segurança, o teste e a revisão de seus resultados, será aplicado depois que as estratégias reativas e proativas forem estabelecidas. A simulação de ataques em um sistema de teste ou laboratório permite avaliar onde há vulnerabilidades e, assim, ajustar as diretivas e os controles de segurança da organização de maneira adequada.

Esses testes não devem ser realizados em um sistema de produção ativo, pois o resultado pode ser desastroso. Dessa forma, a ausência de laboratórios e computadores de teste devido a restrições orçamentárias pode impedir a simulação de ataques. Para garantir os fundos necessários para a realização de testes, é importante que a gerência esteja ciente dos riscos e das conseqüências

de um ataque, assim como das medidas de segurança que podem ser necessárias para proteger o sistema, inclusive os procedimentos de teste. Se possível, todas as situações de ataque devem ser testadas e documentadas fisicamente para se determinar os melhores controles e diretivas de segurança a serem implementados.

Certos ataques, como desastres naturais, não podem ser testados, embora uma simulação ajude. Por exemplo, um incêndio pode ser simulado na sala de servidores, resultando em danos e na perda de todos eles. Essa situação de desastre pode ser útil para testar a capacidade de resposta dos administradores e do pessoal de segurança, bem como para verificar quanto tempo levará para que a organização volte a funcionar.

O ajuste de diretivas e controles de segurança com base nos resultados do teste é um processo iterativo. Ele nunca termina e deve ser avaliado e revisado periodicamente para ser aperfeiçoado.

Operação

Um caminho de escalação e gerenciamento de problemas claramente definido é essencial para um programa de resposta a incidentes. Executando consistentemente o plano de resposta a incidentes logo no início do projeto, as equipes adquirem mais eficiência para resolver problemas em toda a empresa. A documentação dos resultados e o aprendizado adquirido no projeto de segurança são vantajosos para todos que estão começando novos projetos. A coleta desses tipos de lições aprendidas nos processos operacionais facilita a conclusão das tarefas de avaliação, desenvolvimento e implementação do projeto de segurança seguinte.

Resposta a incidentes

Se sua organização desejar implementar totalmente as práticas recomendadas de planejamento de segurança, será necessário criar uma equipe de resposta a incidentes. Essa equipe deve estar envolvida nos esforços proativos para garantir a segurança do sistema. Esses esforços incluem:

- Desenvolver diretrizes para lidar com incidentes.

- Preparar caminhos e procedimentos de escalação para a aplicação de leis relacionadas a crimes de informática.
- Identificar ferramentas de software para resposta a incidentes e eventos.
- Pesquisar e desenvolver outras ferramentas de segurança de computadores.
- Realizar atividades de treinamento e percepção.
- Realizar pesquisas sobre vírus.
- Realizar estudos sobre ataques ao sistema.

Esses esforços fornecerão o conhecimento que a organização poderá usar para resolver questões antes e durante incidentes.
Um administrador de segurança deve poder monitorar e gerenciar auditorias de segurança na organização conforme o necessário. Ele deve ser a autoridade (uma pessoa ou um grupo de pessoas) responsável por implementar a diretiva de segurança para um domínio de segurança. Depois que o administrador de segurança e a equipe de resposta a incidentes concluírem essas funções proativas, o administrador deverá repassar a responsabilidade por lidar com incidentes à equipe de respostas a incidentes.
Isso não significa que o administrador de segurança deva deixar de ser parte da equipe. Contudo, talvez ele não esteja sempre disponível. Portanto a equipe de resposta a incidentes deve ser capaz de lidar com os incidentes sozinha. A equipe será responsável por responder aos incidentes e deverá participar da análise de eventos incomuns que possam envolver a segurança dos computadores ou da rede.

Documentar e aprender
É importante que um ataque seja documentado assim que ocorrer. A documentação deve abordar todos os aspectos conhecidos do ataque, incluindo os danos causados (hardware, software, perda de dados, perda de produtividade),

as vulnerabilidades e os pontos fracos explorados durante o ataque, o tempo de produção perdido, os procedimentos usados para corrigir os danos e o custo dos esforços de correção. A documentação ajudará a modificar estratégias proativas a fim de impedir ataques futuros e minimizar danos.

Implementar planos de contingência

Se os planos de contingência já existirem, eles poderão ser implementados para economizar tempo e para manter as operações do negócio em funcionamento normal. Se não houver um plano de contingência, desenvolva um apropriado com base na documentação da etapa anterior.

Revisar resultados e realizar simulações

Após o ataque ou após defender-se dele, revise o resultado em relação ao sistema e a estratégia proativa da organização. A revisão deve incluir detalhes sobre perda de produtividade, de dados ou de hardware, bem como o tempo gasto para se recuperar do ataque. Você deve realizar simulações em um ambiente de teste que sejam semelhantes ao ambiente de produção para produzir os melhores resultados.

Revisar e ajustar a eficácia das diretivas

Se houver diretivas para defesa contra um ataque que tenha ocorrido, sua eficácia deve ser revisada e verificada. Se não houver diretivas, elas devem ser definidas para minimizar ou impedir ataques futuros.

Quando a eficácia das diretivas existentes não atender ao padrão, as diretivas deverão ser ajustadas apropriadamente. As atualizações de diretivas devem ser coordenadas pelos gerentes pertinentes, o administrador de segurança, os administradores de TI e a equipe de resposta a incidentes. Todas as diretivas devem estar em conformidade com as regras e as diretrizes gerais da organização. Por exemplo, o horário de funcionamento padrão da organização pode ser de 8:00 às 18:00. Uma diretiva de segurança pode ser atualizada ou criada, especificando que os usuários só podem fazer logon no sistema nesse intervalo.

↑_

Disciplina de Gerenciamento de Riscos de Segurança

As seções a seguir se baseiam em práticas comprovadas de metodologias de análise de segurança em uso que aproveitam a MSF e a MOF. A MSF oferece orientações sobre as fases de planejamento, criação, estabilização e implantação do ciclo de vida do projeto nas áreas de arquitetura empresarial e implantação de infra-estrutura. A MOF fornece conselhos sobre como desenvolver ou aperfeiçoar sistemas de gerenciamento de operações de TI. A SRMD é definida em detalhes aqui, o que permite determinar se ela poderá ser aplicada em seu ambiente. A SRMD é um processo detalhado, útil para determinar as ameaças e vulnerabilidades com maior impacto potencial em uma determinada organização.

Identificação de riscos de segurança

A identificação de riscos de segurança é a primeira etapa da avaliação da segurança da organização. Para gerenciar com eficiência os riscos de segurança, isso deve ser declarado com clareza, de forma que a equipe do projeto possa chegar a um consenso e prosseguir para a análise das conseqüências e para a criação de um plano de ação voltado para o risco. Embora o escopo dos riscos de segurança seja limitado à tecnologia que a equipe do projeto tenta proteger, o foco da equipe deve ser amplo o bastante para abordar todas as fontes de riscos de segurança, incluindo tecnologias, processos, ambientes e pessoas.

Os brainstroms são uma maneira de identificar riscos de segurança; há várias fontes de informação sobre questões de segurança na Internet. A organização também pode ter uma avaliação de vulnerabilidade ou um teste de invasão existentes que possam ser revistos para atacar riscos de segurança.

Objetivos

O objetivo da etapa de identificação de riscos de segurança é permitir que a equipe crie uma lista de riscos conhecidos que deixem os ativos da organização em uma posição vulnerável. Essa lista deve ser o mais abrangente possível, abordando todos os pontos de vista da arquitetura empresarial, inclusive tecnologia, negócios, pessoas e estratégia.

O gerenciamento de riscos é o processo de identificação e análise de riscos, e também da criação de um plano para gerenciá-los. Um risco de segurança é

definido como a perda esperada devido a, ou resultante do impacto de, ameaças previstas em relação às vulnerabilidades do sistema e à força e à determinação dos agentes de ameaça relevantes.

Informações

As informações para a etapa de identificação de riscos de segurança incluem a coleta dos conhecimentos disponíveis sobre ameaças; a criação de uma lista de métodos e técnicas de exploração atuais; e a análise de vulnerabilidades das diretivas e do sistema, que possam ser exploradas a fim de causar danos aos ativos da organização. As ameaças incluem qualquer possível perigo às informações e aos sistemas. As vulnerabilidades são os pontos fracos do software, do hardware ou dos procedimentos, que oferecem à ameaça um ponto de ataque. Geralmente, esses riscos originam-se em diferentes pontos do ambiente empresarial, incluindo práticas de negócios, aplicativos, dados e arquitetura da infra-estrutura.

A experiência da equipe, a abordagem atual da organização em relação ao planejamento de segurança na forma de diretivas, procedimentos, diretrizes e modelos, bem como as informações sobre o estado atual da infra-estrutura de tecnologia da organização ajudarão a determinar as informações para esta etapa.

A equipe de segurança pode se basear nas informações obtidas dos próprios ativos ou de resultados de uma ferramenta usada para realizar uma análise de vulnerabilidade ou um teste de invasão. Brainstorms, grupos de discussão e até mesmo workshops formais para coleta de informações sobre as percepções da equipe e dos interessados em relação a questões de segurança se mostrarão úteis para a obtenção de informações.

Atividades de identificação de riscos

Durante a etapa de identificação de riscos de segurança, a equipe procura criar uma declaração ou uma lista de questões de segurança objetiva, descrevendo claramente os riscos enfrentados pela organização. É útil organizar uma série de workshops ou sessões de discussão com a equipe de segurança para identificar os riscos associados à nova situação.

Devido à rápida mudança da tecnologia e dos ambientes, é importante que a identificação de riscos de segurança não seja tratada com uma atividade que deva ser realizada uma única vez. O processo deve ser repetido periodicamente durante o ciclo de vida de operações da organização.

Abordagem estruturada

A utilização de uma abordagem estruturada para o gerenciamento de riscos de segurança é essencial, pois permite que todos os membros da equipe usem um mecanismo consistente para tratar as questões de segurança. O uso de uma classificação de ameaças durante essa etapa é uma maneira útil de fornecer uma abordagem consistente, reproduzível e mensurável.

Classificação de ameaças

As classificações de ameaças (também conhecidas como categorias ou taxonomias) servem a vários propósitos da equipe de segurança. Durante a identificação de riscos, elas podem ser usadas para estimular a discussão sobre riscos de segurança que surgem em diferentes áreas. Durante as sessões de discussão, as classificações também podem reduzir as complexidades de se trabalhar com grandes números de ameaças, pois fornecem uma maneira conveniente de agrupar ameaças semelhantes. As classificações de ameaças também podem ser usadas para fornecer uma terminologia comum que a equipe poderá usar para monitorar e reportar o status de riscos em todo o projeto.

Declaração de risco de segurança

Uma declaração de risco de segurança é uma expressão em linguagem natural sobre a relação causal entre o estado de segurança existente da organização e um resultado de segurança potencial e não concretizado.

A primeira parte da declaração de risco de segurança é chamada de "condição" e fornece a descrição de um estado existente ou de uma possível ameaça que a equipe considere danosa. A segunda parte da declaração de risco é chamada de "conseqüência" e descreve a perda indesejável de confidencialidade, integridade e disponibilidade de um ativo.

As duas declarações são ligadas por um termo como "então" ou "poderá resultar em", que sugere uma relação incerta (em outras palavras, menor que 100%) ou causal.

Os seguintes itens apresentam a declaração de risco usada neste guia:

SE um *Agente de Ameaça* usar uma ferramenta, uma técnica ou um método para explorar uma *Vulnerabilidade*, **ENTÃO** a perda de (confidencialidade, integridade ou disponibilidade) de um *ativo* poderá resultar em um impacto.

As declarações de risco de segurança são desenvolvidas por meio da análise de riscos. Há dois tipos de abordagem de análise de riscos: qualitativa e quantitativa. Nenhuma dessas abordagens é melhor que a outra: cada uma fornece uma ferramenta valiosa para a estruturação das atividades de identificação de riscos. A abordagem quantitativa se baseia nas informações coletadas no processo quantitativo.

Figura 2

Declaração de risco de condição e conseqüência da segurança

As seguintes etapas detalham cada parte do processo da figura mostrada acima:

1. Defina uma declaração de risco de condição e conseqüência para cada ameaça.

   Se um agente concluir uma ameaça e explorar uma vulnerabilidade, o ataque levará a um risco. O ataque pode danificar o ativo ao reduzir a confidencialidade, a integridade ou a disponibilidade. Portanto, ele causa a

exposição da empresa a perdas. Contudo, essas exposições podem ser combatidas por salvaguardas.

2. Atribua uma probabilidade de ameaça (PA) (0% mais baixa – 100% mais alta). A probabilidade de ameaça é a probabilidade de um possível agente de ameaça entrar no ambiente.
3. Atribua um fator de criticalidade (FC) (1 mais baixo – 10 mais alto). O fator de criticalidade é o nível de exploração potencial da ameaça a um ativo.
4. Classifique o esforço (E) (1 mais baixo – 10 mais alto). O esforço representa as habilidades necessárias para que um atacante tire vantagem da exploração.
5. Determine o fator de risco (FR). É o fator de criticalidade dividido pelo esforço.
6. Determine o nível de freqüência da ameaça usando a equação (PA × FR).
7. Classifique o fator de vulnerabilidade (FV) (1 mais baixo – 10 mais alto). Decida o tamanho do risco imposto pela vulnerabilidade a um ativo.
8. Determine a prioridade do ativo (PrA) (1 mais baixa – 10 mais alta). Determine a classificação da prioridade de cada ativo da empresa com base nos critérios a seguir. A atribuição de valores dos ativos é um processo complexo e pode levar tempo para ser aperfeiçoada. Para obter mais informações sobre atribuição de valores de ativos, consulte as referências a esse assunto no fim deste módulo. Priorizar os ativos da organização é fundamental para determinar quantos ativos podem ser protegidos com o orçamento disponível.

   Para obter ajuda ao formular uma lista de ativos prioritários, pesquise respostas às seguintes questões sobre cada ativo com base no ambiente da organização:

   - Qual é o valor do ativo para a empresa?
   - Quanto custa a manutenção ou a proteção do ativo?

- Quanto o ativo gera de lucros para a empresa?
- Quanto o ativo valeria para os concorrentes?
- Quanto custaria a recriação ou a recuperação do ativo?
- Quanto custou a aquisição ou o desenvolvimento do ativo?

9. Determine o fator de impacto (FI) usando a equação (FV × PrA).
10. Determine o fator de exposição (FE) usando a equação (Nível de Freqüência da Ameaça × Fator de Impacto dividido por 1.000). O fator de exposição é expresso como uma porcentagem para que seja possível calcular a expectativa de perda única (EPU) nas etapas que continuam na tabela 2.

O processo de formulação em duas partes usado para produzir declarações de risco de segurança tem a vantagem de unir as conseqüências possíveis em um ativo às condições observáveis (e potencialmente controláveis) que existem atualmente na organização. Abordagens alternativas em que a equipe se concentra somente nas condições de riscos identificáveis podem exigir que a equipe redefina a condição de risco posteriormente no processo de análise de riscos de segurança, quando as estratégias de planejamento de gerenciamento de riscos de segurança são criadas.

Observação: declarações de risco de segurança não são puramente declarações do tipo "se-então"; elas são declarações de fato que exploram as possíveis, mas não concretizadas, conseqüências de um risco.

Pode ser útil considerar declarações "se-então" hipotéticas a fim de comparar as alternativas e formular planos por meio de árvores de decisão. No entanto, seu objetivo durante a fase de identificação de riscos de segurança é simplesmente identificar o máximo possível de riscos de segurança. Adie a decisão de como analisá-los e gerenciá-los para uma fase posterior do processo.

A declaração de risco de segurança criada deve incluir condições e conseqüências. Como parte de uma análise profunda de riscos de segurança, os membros da equipe devem procurar semelhanças e agrupamentos naturais das condições das questões de segurança e, em seguida, redefinir as relações de cada uma delas em busca de uma causa raiz comum. Também vale a pena redefinir as ramificações das relações a partir da causa raiz da condição, assim que ela for conhecida. Isso examinará os efeitos nos ativos de fora da organização para que seja possível obter uma melhor avaliação das perdas totais ou das oportunidades perdidas associadas à ameaça de segurança.

Durante a identificação de riscos de segurança, não é difícil encontrar a mesma condição associada a várias conseqüências. No entanto, o oposto também pode ser verdadeiro: pode haver diversas condições que produzam a mesma conseqüência. Às vezes, a conseqüência de um risco de segurança identificado em uma área da organização pode se tornar uma condição de risco em outra área. Essas situações devem ser registradas para que decisões apropriadas sejam tomadas durante a análise e o planejamento de riscos de segurança a fim de se levar em conta as dependências e as relações entre os riscos de segurança.

Dependendo das relações entre os riscos de segurança na organização, atenuar um único risco pode resultar na atenuação de um grupo inteiro de riscos dependentes e, assim, na alteração de todo o perfil de risco da organização. Documentar essas relações logo no início da fase de identificação de riscos de segurança pode fornecer informações úteis para a condução de um planejamento de riscos de segurança que seja flexível, abrangente e eficiente no exame de recursos necessários para a abordagem das causas raiz ou ramificadas. Para os riscos de segurança mais importantes, os benefícios do registro de tais informações adicionais na etapa de identificação devem ser comparados com a rapidez com que se passa pela análise e pela priorização subseqüentes e com o novo exame das dependências e das causas raiz durante a fase de planejamento.

Atribuindo valores aos ativos na organização

Determinar o valor monetário de um ativo é uma parte importante do gerenciamento de riscos. Com freqüência, os gerentes de negócios contam com o valor de um ativo para ajudá-los a determinar quanto dinheiro e tempo devem

gastar para protegê-lo. Diversas organizações mantêm uma lista de valores patrimoniais como parte de seus planos de recuperação de desastres. O uso do modelo de atribuição de valores a seguir ajudará a organização a determinar como deve priorizar os ativos, conforme detalhado na etapa 8 da análise quantitativa.

Para atribuir adequadamente um valor a um ativo, calcule estes três valores principais:

- O valor geral do ativo para a organização. Calcule ou estime o valor do ativo em termos financeiros diretos. Por exemplo, se houver um site de comércio eletrônico que funcione normalmente a semana toda, 24 horas por dia, e gere uma receita média de R$ 2.000 por hora em pedidos de clientes, você poderá declarar com segurança que o valor anual do site em temos de receitas de vendas é de R$ 17.520.000.
- O impacto financeiro imediato da perda do ativo. Se o mesmo site ficar indisponível por seis horas, a exposição calculada será de 0,000685% ao ano. Se multiplicar essa porcentagem de exposição pelo valor anual do ativo, você poderá prever que as perdas diretamente relacionadas neste caso seriam de R$ 12.000.
- O impacto de negócios indireto da perda do ativo. Neste exemplo, a empresa estima que gastaria R$ 10.000 em propaganda para contrabalançar a publicidade negativa de tal incidente. Além disso, a empresa também estima uma perda de 0,01% a 1% das vendas anuais, ou R$ 17.520. Ao combinar as despesas publicitárias extras e a perda de receita de vendas anual, você poderá prever um total de R$ 27.520 em perdas indiretas neste caso.

Tabela 1: Exemplo de atribuição de valores de ativos

Ativo	**Valor**	**Fator de exposição**	**Impacto direto**	**Impacto indireto**
Site de comércio eletrônico	R$ 17.520.000 por ano	Seis horas por ano ou 0,000685	R$ 12.000	R$ 27.520

Você também deve levar em consideração o valor do ativo para seus concorrentes. Por exemplo, se seus concorrentes puderem usar informações de clientes obtidas anteriormente no site enquanto este estiver inativo, você poderá perder milhões em receita para eles.

Há vários métodos e equações que podem ser usados para a realização de uma análise de riscos quantitativa e há diversas variáveis que podem ser inseridas no processo. No entanto, estas etapas adicionais são continuações da etapa 10 acima que devem ser seguidas para a obtenção de uma análise de riscos de segurança quantitativa:

1. Determine a expectativa de perda única (EPU). É a quantidade total de receita perdida em uma única ocorrência do risco. A EPU é um valor atribuído a um único evento que representa o possível valor de perda da empresa caso uma ameaça específica ocorra. Calcule a EPU multiplicando o valor do ativo (VA) pelo fator de exposição (FE). A EPU é semelhante ao impacto de uma análise de riscos qualitativa Determine a EPU usando a equação (VA × FE).
   O fator de exposição representa a porcentagem de perda que uma ameaça concretizada pode ter em um determinado ativo. Se uma Web farm tiver um valor patrimonial igual a R$ 150.000 e um incêndio resultar em danos estimados em 25% do valor, a EPU será de R$ 37.500. Esse valor é calculado para ser inserido na equação de EPA da etapa 3.
2. Determine a taxa de ocorrência anual (TOA). A TOA é o número de vezes que você espera que o risco ocorra durante o ano. Para estimar a TOA, baseie-se em sua experiência e consulte especialistas em gerenciamento de riscos, assim como consultores de segurança e de negócios. A TOA é semelhante à probabilidade de uma análise de riscos qualitativa. O intervalo da TOA varia de 0% (nunca) a 100% (sempre).
   Por exemplo, se um incêndio na Web farm da mesma empresa resultar em danos de R$ 37.500 e a probabilidade, ou TOA, de ocorrer um incêndio for de 0,1 (indicando uma vez a cada dez anos), o valor da EPA neste caso será de R$ 3.750 (R$ 37.500 x 0,1 = R$ 3.750).
3. Determine a expectativa de perda anual (EPA). A EPA é a quantidade total de dinheiro que a organização perderá em um ano se nada for feito para atenuar o risco. Calcule esse valor multiplicando a EPU pela TOA. A EPA é semelhante à classificação relativa de uma análise de riscos qualitativa. Determine a EPA usando a equação (TOA × EPU).

A EPA fornece um valor com o qual a empresa pode trabalhar para orçar o custo do estabelecimento de controles ou salvaguardas para impedir esse tipo de dano — neste caso, R$ 3.750 ou menos por ano — e fornecer um nível adequado de proteção. É importante quantificar a possibilidade real de um risco e quantos danos, em termos monetários, a ameaça poderá causar para saber quanto pode ser gasto para proteger contra as possíveis conseqüências da ameaça.

4. Estime o custo de contramedidas ou salvaguardas usando a seguinte equação:
(EPA antes da contramedida) – (EPA depois da contramedida) – (custo anual da contramedida) = valor da salvaguarda para a empresa (VSE)
Por exemplo, a EPA de que um atacante desative um servidor Web é R$ 12.000 e, após a salvaguarda ser implementada, a EPA é avaliada em R$ 3.000. O custo anual de manutenção e operação da salvaguarda é R$ 650; portanto, o valor dessa salvaguarda é R$ 8.350 por ano, conforme expresso pela seguinte equação: (R$ 12.000 - R$ 3.000 - R$ 650 = R$ 8.350).

Os itens de informação da análise de riscos quantitativa fornecem objetivos e resultados claramente definidos. O resumo a seguir define o que geralmente é obtido dos resultados das etapas anteriores:

- Valores monetários atribuídos aos ativos.
- Uma lista abrangente de ameaças significativas.
- A probabilidade de ocorrência de cada ameaça.
- A possível perda para a empresa com base em cada ameaça ao longo de doze meses.
- Salvaguardas, contramedidas e ações recomendadas.

Resultados

O resultado mínimo das atividades de identificação de riscos de segurança é uma declaração de consenso clara e objetiva dos riscos enfrentados pela equipe de segurança, documentados como a lista de questões de segurança. A lista de questões de segurança, em forma de tabela, é o resultado principal para a fase seguinte do processo de gerenciamento de riscos de segurança — a análise.

Com freqüência, a etapa de identificação de riscos de segurança gera uma grande quantidade de outras informações úteis, incluindo a identificação de causas raiz e efeitos ramificados, partes afetadas, proprietários etc.

É recomendável manter um registro em forma de tabela contendo as declarações de risco de segurança e as informações de causas raiz e efeitos ramificados que a equipe de segurança desenvolve. Informações adicionais para a classificação dos riscos de segurança por ameaça também poderão ser úteis quando as informações de riscos de segurança forem utilizadas para criar ou usar uma base de conhecimento de segurança se existir uma taxonomia bem definida para a organização.

Estas são outras informações que talvez a equipe de segurança deseje registrar durante o processo de identificação de riscos:

- Restrições
- Circunstâncias
- Suposições
- Fatores contribuintes
- Dependências entre riscos de segurança
- Questões relacionadas
- Proprietários dos ativos da empresa

- Preocupações da equipe

Análise e priorização dos riscos de segurança

A análise e a priorização de riscos de segurança é a segunda grande etapa no processo de avaliação de segurança. A análise de riscos de segurança envolve a conversão de dados de riscos de segurança (ameaças, explorações e vulnerabilidades) em um formulário para facilitar a tomada de decisões. A priorização de riscos de segurança garante que os membros da equipe de segurança resolverão os riscos de segurança mais importantes primeiro.

Durante esta etapa, a equipe de segurança examina os itens da lista de questões de segurança produzida na etapa de identificação de riscos de segurança a fim de priorizá-los e formar um Plano de Ação de Segurança.

No Plano de Ação de Segurança, a equipe de segurança da organização pode usar a lista de questões de segurança a fim de planejar e confirmar recursos para a execução de uma estratégia específica voltada para o gerenciamento das questões no ambiente.

A equipe também pode identificar que questões de segurança, se houver, podem ser retiradas da lista por terem uma prioridade muito baixa para ação. À medida que essa fase de implementação de segurança caminha para a conclusão e o ambiente da organização muda, a identificação de riscos de segurança e a análise de riscos de segurança devem ser repetidas para que a eficácia do plano de ação de segurança seja validada. Novos riscos de segurança podem surgir e antigos riscos, que não mais apresentem uma prioridade suficientemente alta, podem ser removidos, descontados ou "desativados".

Objetivo

O principal objetivo da etapa de análise de riscos de segurança é priorizar as questões de segurança do Plano de Ação de Segurança a fim de determinar quais delas garantem a confirmação de recursos da organização para atenuá-las.

Informações
Durante o processo de análise de riscos, a equipe se baseará em sua própria experiência e nas informações derivadas de outras fontes relevantes relacionadas às declarações de risco de segurança. Consulte as diretivas e os procedimentos de segurança da organização, os bancos de dados de conhecimento sobre segurança do setor, as análises de vulnerabilidade, as simulações de segurança e os proprietários dos ativos para obter informações sobre como transformar declarações de risco de segurança brutas em uma lista mestra de riscos priorizados.

Atividades de análise de riscos de segurança
Há diversas técnicas qualitativas e quantitativas usadas para a realização da priorização em um Plano de Ação de Segurança. Uma técnica fácil para a análise de riscos de segurança é usar estimativas de consenso da equipe derivadas de dois componentes de risco amplamente aceitos: probabilidade e impacto. É possível multiplicar esses valores estimados para calcular uma única estatística chamada de exposição ao risco.

Probabilidade do risco de segurança
A probabilidade do risco de segurança é uma medida da probabilidade de que o estado de negócios descrito na parte de condição de riscos da declaração de risco de segurança realmente ocorra. A declaração de risco pode incluir outros fatores além de tempo e dinheiro da empresa, como os descritos na seguinte parte da declaração de risco:
"**SE** um *Agente de Ameaça* usar uma *ferramenta, uma técnica ou um método* para explorar uma *Vulnerabilidade*..."
A ameaça que usa uma exploração para tirar proveito de uma vulnerabilidade é a parte de condição da declaração de risco. Para determinados tipos de ameaça, pode não haver uma exploração ou uma vulnerabilidade conhecida, especialmente quando a ameaça é um desastre natural.
Para classificar os riscos, é desejável que um valor numérico seja atribuído à probabilidade do risco. Se a probabilidade do risco de segurança não for maior do que zero, a ameaça não representará uma questão de segurança. Se a

probabilidade for 100%, o risco de segurança será uma certeza e poderá ser uma questão conhecida.

As probabilidades são notoriamente difíceis de se estimar e aplicar, embora bancos de dados de riscos do setor ou da empresa possam ser úteis para fornecer estimativas de probabilidade conhecidas com base em amostras de um grande número de projetos. No entanto, como as equipes do projeto podem expressar suas experiências em termos de linguagem natural, pode ser útil mapear esses termos a intervalos de probabilidades numéricas, conforme demonstrado na tabela a seguir.

Tabela 2: Probabilidade do risco

Intervalo	Valor de cálculo	Expressão	Pontuação
1% a 14%	7%	Muito improvável	1
15% a 28%	21%	Baixa	2
28% a 42%	35%	Improvável	3
43% a 57%	50%	50 – 50	4
58% a 72%	65%	Provável	5
73% a 86%	79%	Altamente provável	6
87% a 99%	93%	Quase certo	7

O valor de probabilidade usado para cálculo representa o meio de um intervalo. Com a ajuda dessas tabelas de mapeamento, um método alternativo para quantificar a probabilidade é relacionar o intervalo de probabilidade ou a expressão de linguagem natural combinada pela equipe a uma pontuação numérica. Se uma pontuação numérica for usada para representar o risco de segurança, será necessário usar a mesma pontuação para todos os riscos de segurança para que o processo de priorização funcione com eficiência.

Independentemente da técnica usada para quantificar a incerteza, a equipe sempre precisará desenvolver uma abordagem para derivar um único valor da probabilidade do risco que represente o consenso para cada risco.

Impacto do risco de segurança

O impacto do risco é uma estimativa da criticalidade da perda causada por efeitos adversos nos ativos ou a magnitude de uma perda resultante da perda da

confidencialidade, da integridade ou da disponibilidade de um ativo. Ele deve ser uma medida direta das conseqüências de segurança, conforme definido na segunda parte da declaração de risco de segurança:

"...**ENTÃO** uma perda de (confidencialidade, integridade ou disponibilidade) de um *Ativo* poderá resultar em um impacto.

A perda pode ser medida em termos financeiros ou em uma escala subjetiva em relação ao ativo. Se todos os impactos de riscos de segurança puderem ser expressos em termos financeiros, o uso do valor financeiro para quantificar a magnitude da perda ou o custo de oportunidade terá a vantagem de ser conhecido pelos patrocinadores do negócio. O impacto financeiro pode consistir nos custos de longo prazo em operações e suporte, na perda de participação no mercado, nos custos de curto prazo em trabalho adicional ou no custo da oportunidade.

Em outras situações, uma escala subjetiva de 1 a 5 ou de 1 a 10 é mais apropriada para medir o impacto do risco de segurança. Um exemplo de quando uma escala subjetiva pode ser usada seria uma situação em que o valor líquido apropriado dos ativos não pode ser determinado com rapidez. Desde que todos os riscos de segurança de um Plano de Ação de Segurança usem as mesmas unidades de medida, as técnicas simples de priorização serão boas o suficiente.

Tabela 3: Exemplo de sistema de pontuação de perda de ativo

Pontuação	**Perda monetária**
1	Abaixo de R$ 100
2	R$ 100 – R$ 1.000
3	R$ 1.000 – R$ 10.000
4	R$ 10.000 – R$ 100.000
5	R$ 100.000 – R$ 1 milhão
6	R$ 1 milhão – R$ 10 milhões
7	R$ 10 milhões – R$ 100 milhões
8	R$ 100 milhões – R$ 1 bilhão
9	R$ 1 bilhão – R$ 10 bilhões
10	Acima de R$ 10 bilhões

O sistema de pontuação para a estimativa do impacto varia entre as organizações e deve refletir os valores e as diretivas da sua organização. Por exemplo, uma perda monetária de R$ 10.000 pode ser tolerável para uma equipe ou organização, mas inaceitável para outra. A pontuação de um impacto catastrófico com um valor artificialmente alto, como 100, garantirá que até mesmo um risco com uma probabilidade muito baixa chegue ao topo da lista de riscos e permaneça lá.

Exposição ao risco de segurança

A exposição ao risco mede o risco de segurança geral para os ativos, combinando informações que expressam a probabilidade de perda real com informações que expressam a magnitude da possível perda em uma única estimativa numérica. A equipe de segurança pode, então, usar a magnitude da exposição ao risco para classificar questões de segurança. Na forma mais simples de análise de riscos quantitativa, a exposição ao risco é calculada multiplicando-se a probabilidade do risco pelo impacto.

Quando as pontuações são usadas para quantificar a probabilidade e o impacto, às vezes é conveniente criar uma matriz que considere as possíveis combinações de pontuações e as atribua a categorias de risco baixo, médio e alto. Usando uma pontuação de probabilidade tríplice, onde 1 é baixo e 3 é alto, e uma pontuação de impacto tríplice, onde 1 é baixo e 3 é alto, os resultados podem ser expressos na forma de uma tabela em que cada célula é um valor possível para a exposição ao risco. Com esta organização, é fácil classificar riscos como baixos, médios e altos, dependendo de sua posição nas faixas diagonais da pontuação crescente.

Tabela 4: Matriz de pontuação de risco

Impacto da probabilidade	**Baixo = 1**	**Médio = 2**	**Alto = 3**
Alto = 3	3	6	9
Médio = 2	2	4	6
Baixo = 1	1	2	3
Intervalos de exposição: Baixo =1 – 2; Médio =3 – 4; Alto = 6 – 9			

A vantagem é que esse formato tabular permite que os níveis de riscos de segurança sejam incluídos em relatórios de status a serem enviados para os

patrocinadores e interessados, que possibilitam a utilização de cores (vermelho para a zona de risco alto no canto superior direito, verde para o risco baixo no canto inferior esquerdo e amarelo para níveis de risco médio ao longo da diagonal). Uma terminologia bem definida e de fácil compreensão melhora a comunicação desses valores, pois é mais fácil compreender "alto risco" do que "alta exposição".

Técnicas quantitativas adicionais

Como os objetivos da análise de riscos de segurança são priorizar os riscos de segurança, realizar um Plano de Ação de Segurança e orientar as decisões relacionadas à confirmação de recursos para gerenciamento de segurança, a equipe de segurança deve selecionar um método de priorização dos riscos que seja adequado para o projeto, para a equipe e para os interessados.

Algumas organizações se beneficiam do uso de técnicas ponderadas e com vários atributos para levar em conta outros componentes que a equipe deseja considerar no processo de classificação, como o prazo exigido, a magnitude do possível ganho de oportunidade, a confiabilidade das estimativas de probabilidade e a atribuição de valores física ou informativa dos ativos.

A seleção do método "certo" ou da combinação "certa" de métodos de análise de riscos de segurança depende do equilíbrio adequado entre o esforço para realizar a análise de riscos de segurança e a escolha de priorização incorreta ou indefensável (para os interessados) no Plano de Ação de Segurança. A análise de riscos de segurança deve ser realizada para dar suporte à priorização que orienta a tomada de decisões e nunca deve ser feita simplesmente por ser feita.

Os resultados das abordagens quantitativas ou semi-quantitativas para a priorização de riscos de segurança devem ser avaliados no contexto das diretrizes de negócios, diretivas e procedimentos, dados e infra-estruturas de tecnologia. Uma abordagem semi-quantitativa começa com algum tipo de medida qualitativa para permitir que as empresas apresentem medidas de segurança quantificáveis.

Resultados

A análise de riscos de segurança fornece à equipe uma lista de ações de segurança priorizadas para orientar a realização das atividades de planejamento de riscos de segurança. Com freqüência, as informações de riscos de segurança detalhadas, incluindo condições, contexto, causas raiz e estatísticas usadas para priorização (probabilidade, impacto, exposição), são registradas para cada risco no formulário de declaração de risco, que será descrito em detalhes posteriormente neste módulo.

Lista mestra de riscos de segurança

A lista dos principais riscos de segurança para os quais deve ser criado um plano de ação é definida no Plano de Ação de Segurança. Esse plano identifica a condição que causa o risco de segurança, o possível efeito adverso (conseqüência) e também os critérios ou as informações usados para classificar o risco, como sua probabilidade, seu impacto e sua exposição. Um exemplo de lista mestra de riscos que usa a abordagem de estimativa de dois fatores (probabilidade e impacto) é mostrada aqui.

Tabela 5: Exemplo de lista mestra de riscos e priorização

Prioridade	Condição	Conseqüência	Probabilidade	Impacto	Exposição
1	Vírus infectando site de comércio eletrônico	Seis horas para recriar o servidor.	80%	3	2,4
2	Nenhum padrão de codificação para nova linguagem de programação	Lançar com potencialmente mais vulnerabilidades de segurança.	45%	2	0,9
3	Nenhuma especificação escrita	Alguns recursos de segurança do produto não implementados	30%	2	0,6

Exposição calculada como probabilidade x impacto. Impacto baixo = 1, impacto médio = 2 e impacto alto = 3.

A lista mestra de riscos de segurança é a compilação de todas as informações de avaliação de riscos de segurança. É um documento ativo que forma a base do processo contínuo de gerenciamento de riscos de segurança e deve ser mantido atualizado em todo o ciclo de vida de TI que inclua avaliação, planejamento, criação, implantação e operação.

A lista mestra de riscos de segurança é o documento fundamental para dar suporte ao gerenciamento de riscos proativo ou reativo. Ela permite a tomada de decisões de equipe ao fornecer a base para:

- Priorização de esforços.
- Identificação de ações críticas.
- Realce de dependências.

O método usado para calcular a exposição criada por um risco deve ser documentado cuidadosamente no plano de gerenciamento de riscos e é preciso tomar cuidado para garantir que os cálculos registrem com precisão as intenções da equipe, ponderando a importância dos diferentes fatores.

Para identificar ameaças aos ativos, realize análises de riscos. Para cada tipo de ameaça identificada, crie uma declaração de risco. As declarações de risco combinam informações sobre uma ameaça a informações sobre o impacto da ameaça, caso ocorra.

Tabela 6: Conteúdo da lista mestra de riscos de segurança

Item	Objetivo	Status
Declaração de risco de segurança	Articular claramente o risco.	Obrigatório
Probabilidade	Quantificar a probabilidade de ocorrência da ameaça.	Obrigatório
Impacto	Quantificar a criticalidade da perda ou a	Obrigatório

Item	Objetivo	Status
	magnitude do custo da oportunidade.	
Critério de classificação	Medida única da importância.	Obrigatório
Prioridade (classificação)	Priorizar ações.	Obrigatório
Proprietário	Garantir o acompanhamento dos planos de ação de riscos.	Obrigatório
Plano de atenuação	Descrever medidas preventivas.	Obrigatório
Disparadores e plano de contingência	Descrever medidas corretivas.	Obrigatório
Causas raízes	Guiar um planejamento de intervenção eficiente.	Obrigatório
Efeitos ramificados	Garantir estimativas de impacto adequadas.	Opcional
Contexto	Documentar informações históricas para registrar a intenção da equipe de identificar riscos.	Opcional
Tempo para implementação	Registrar a importância de que os controles de risco sejam implementados em um determinado prazo.	Opcional

Formulário de declaração de risco

Ao analisar cada risco de segurança individualmente, ou durante as atividades de planejamento de segurança relacionadas a uma ameaça, uma exploração ou uma vulnerabilidade específica, é conveniente ver todas as informações sobre esse risco de segurança em um documento, chamado de formulário de declaração de risco de segurança. Para obter mais detalhes sobre os processos de um projeto de segurança, consulte o guia *Microsoft Solution for Security Services*.

Normalmente, uma lista de declarações de risco de segurança contém os campos da lista mestra de riscos de segurança criada durante as fases de identificação e avaliação e poderá ser aumentada se a equipe inserir informações adicionais importantes durante o processo de gerenciamento de riscos de segurança. Poderá

ser mais fácil tratar a lista de declarações de risco de segurança como um documento separado da lista mestra de riscos se os riscos forem atribuídos à equipe de segurança para ações de acompanhamento. Estas são algumas das informações que a equipe deve levar em consideração ao desenvolver um formulário de declaração de risco:

Tabela 7: Formulário de declaração de risco

Item	Objetivo
Identificador do risco de segurança	Nome usado pela equipe para identificar riscos exclusivamente para fins de relatório e controle.
Origem do risco de segurança	Uma abrangente classificação da área subjacente da qual o risco de segurança se originou. Usado para identificar áreas onde causas raízes recorrentes do risco de segurança devem ser pesquisadas.
Condição do risco de segurança (ameaça/exploração)	Frase que descreve a condição existente que pode levar a uma perda. Forma a primeira parte de uma declaração de risco de segurança.
Conseqüências do risco (vulnerabilidade/impacto no ativo)	Frase que descreve a perda que poderá ocorrer se um risco tiver uma conseqüência. Forma a segunda parte de uma declaração de risco de segurança.
Probabilidade do risco de segurança	Probabilidade maior que zero e menor que 100% que representa a possibilidade de uma condição de risco realmente ocorrer, resultando em uma perda.
Classificação de impacto no ativo	Abrangente classificação do tipo de impacto que pode ser produzido por um risco.
Exposição do ativo	Ameaça geral do risco, comparando a possibilidade de perda real com a magnitude da perda em potencial. A equipe usa a exposição para classificar riscos. Para calcular a exposição é necessário multiplicar a probabilidade pelo impacto do risco.

Item	Objetivo
Contexto do risco	Parágrafo que contém informações históricas que ajudam a esclarecer a situação do risco de segurança.
Riscos de segurança relacionados	Lista de identificadores de risco usada pela equipe para controlar riscos interdependentes.

Lista dos principais riscos de segurança

A análise dos riscos de segurança avalia a ameaça de cada risco de segurança para ajudar a equipe a decidir que problema requer uma ação. O gerenciamento de segurança e o planejamento associado a ele são tarefas demoradas e trabalhosas que roubam o tempo que poderia ser gasto em outras atividades; portanto, é importante que a equipe de segurança faça tudo o que for necessário para proteger os ativos mais valiosos.

Uma técnica simples mas eficaz de monitoramento de riscos de segurança é criar uma lista dos principais riscos de segurança contendo as questões mais críticas. Essa lista poderá ficar externamente visível para todos os participantes. Desse modo, ela poderá ser usada em outros projetos de TI ativos em que a segurança possa ser afetada.

A organização precisa determinar qual será o conteúdo da lista dos principais riscos de segurança com base em diversos fatores, inclusive tempo, recursos e ativos. Depois de selecionar que riscos de segurança precisam ser gerenciados, você deve alocar recursos de equipe para desenvolver planos que englobem esses riscos.

Depois de classificar os riscos de segurança, a equipe deve concentrar-se em uma estratégia de gerenciamento para esses riscos e em um modo de incorporar os planos de ação de segurança ao plano geral de avaliação de segurança.

Desativando riscos de segurança

Os riscos de segurança podem ser desativados ou classificados como inativos para que a equipe se concentre em outros problemas que exijam gerenciamento mais proativo. Classificar um risco de segurança como inativo significa que a equipe de avaliação decidiu que esse risco não vale o esforço necessário para

controlar a ameaça específica no momento. A decisão de desativar um risco de segurança é tomada durante a análise de risco.
Alguns riscos de segurança são desativados porque a probabilidade de sua ameaça é praticamente zero e é possível que permaneça assim devido a suas condições extremamente improváveis. Outros riscos de segurança são desativados porque seu impacto nos ativos está abaixo do limite em que vale a pena despender esforços para planejar uma atenuação proativa ou uma estratégia de contingência reativa. Nesses casos, é simplesmente mais econômico sofrer as possíveis conseqüências desses riscos de segurança.
Não é aconselhável desativar riscos de segurança acima desse limite de impacto no ativo, mesmo que sua exposição seja baixa, a não ser que a equipe de segurança esteja certa de que a probabilidade (e portanto, a exposição) permanecerá baixa em todas as circunstâncias previsíveis. Lembre-se de que desativar um risco de segurança não é o mesmo que resolvê-lo. Um risco de segurança desativado poderá reaparecer sob determinadas condições e a equipe de segurança poderá optar por reclassificá-lo como ativo e reiniciar as atividades de avaliação de riscos de segurança.

Controlando, planejando, agendando e relatando riscos de segurança

Controlar os riscos de segurança identificados no Plano de Ação de Segurança e implementar um processo de planejamento, agendamento e criação de relatórios para remediá-los são as próximas etapas do processo. Com base nas prioridades identificadas na etapa anterior, a equipe fará alterações de forma proativa, modificando a infra-estrutura de tecnologia e implementando novos processos e procedimentos de segurança.
Quando um risco não pode ser gerenciado de forma proativa, um plano reativo é gerado e executado quando um evento é acionado. Após a criação dos planos, é produzido um agendamento de implementação para as modificações propostas. Por fim, várias tarefas de correção são atribuídas a membros da equipe.
O agendamento envolve a integração das tarefas necessárias à implementação dos planos de ação de segurança na agenda do projeto de avaliação. Isso é feito por meio da atribuição a indivíduos e controle ativo de seus status.

A criação de relatórios consiste na redefinição de riscos que mudaram porque o escopo e a definição do projeto e dos processos foram alterados. Esse tipo de relatório também é conhecido como gerenciamento de alterações de risco. A criação de relatórios também consiste no fechamento de riscos de segurança a partir dos principais riscos gerenciados de um projeto. A figura a seguir ilustra toda essa etapa.

Figura 3

Controlando, planejando, agendando e relatando riscos

Objetivos

O objetivo principal da etapa de planejamento e agendamento de riscos de segurança é desenvolver planos de ação detalhados para controlar os principais riscos de segurança identificados durante a análise e integrar esses planos aos processos padrão de gerenciamento de projeto a fim de garantir que sejam concluídos.

Informações

O planejamento de riscos de segurança deve estar totalmente integrado à infra-estrutura e aos processos padrão de planejamento de projetos. É importante observar que há riscos associados ao próprio projeto de avaliação de segurança, mas esses riscos são diferentes dos riscos de segurança reais. A implementação de planos de ação de segurança leva risco ao projeto geral e deve ser gerenciada com a metodologia da RMD da MSF. Normalmente, os riscos do projeto em relação à implementação do Plano de Ação de Segurança incluem tempo, dinheiro e recursos.

As informações relacionadas ao processo de planejamento de riscos de segurança incluem não somente a lista mestra de riscos de segurança, a lista dos principais riscos de segurança e as informações do knowledge base de segurança, mas também os planos de ação de segurança e os agendamentos de implementação de segurança.

Atividades de planejamento

Ao desenvolver planos para reduzir a exposição dos ativos, você deve:

- Concentrar-se em riscos de segurança de exposição alta.
- Abordar a condição de ameaça (ameaça, explorações) para reduzir a probabilidade.
- Procurar causas raízes da questão de segurança em vez de sintomas.
- Abordar as conseqüências sobre o ativo (vulnerabilidade e ativo) para minimizar o impacto no ativo.
- Determinar a causa raiz da questão de segurança e procurar situações semelhantes resultantes da mesma causa que possam afetar os mesmos ou outros ativos.
- Ficar atento às dependências e interações de ameaças, explorações e vulnerabilidades entre riscos de segurança.

Existem diversas abordagens de planejamento para reduzir diferentes condições de risco de projeto. Essas abordagens incluem:

- Para riscos de projeto que possam ser controlados pela equipe, aplique os recursos de equipe necessários para a redução da probabilidade da condição de ameaça. Essa abordagem de gerenciamento de riscos de segurança é proativa.
- Para riscos de projeto fora do controle da equipe, encontre uma possível solução temporária ou transfira (escale) o risco de segurança para pessoas que tenham autoridade para intervir.
- Para riscos de projeto fora do controle da equipe que não possam ser transferidos ou gerenciados proativamente, e equipe deve desenvolver planos para minimizar o impacto no ativo ou sua perda. Essa abordagem de

gerenciamento de riscos de segurança é reativa.

Planejamento de ações de segurança

Existem seis abordagens principais para o planejamento de ações de segurança e sua equipe deve considerar os problemas associados a cada uma delas, listadas aqui resumidamente, ao formular o plano de ação de riscos de segurança. As abordagens são definidas mais detalhadamente a seguir.

- **Pesquisa**. A equipe de segurança sabe o bastante sobre o risco de segurança? Você precisa estudar mais a ameaça, a exploração, a vulnerabilidade ou os ativos para determinar melhor as características desses componentes antes de decidir que ação deve ser executada?
- **Aceitação**. Você está disposto a aceitar o risco e não executar nenhuma ação proativa, com exceção dos planos de contingência? Talvez você deva considerar aceitar um risco se o valor de EPA do ativo for menor que o valor do ativo e se o impacto nos negócios for baixo. Sua organização poderá suportar as conseqüências se o risco de segurança realmente ocorrer?
- **Evitar Riscos**. Há uma maneira de evitar riscos eliminando a fonte do risco ou a exposição de um ativo ao risco? Esta é uma reação extrema e só deve ser realizada quando o impacto do risco for maior que o benefício obtido com o ativo. A organização pode evitar riscos alterando o escopo do projeto de implementação?
- **Transferência**. É possível transferir riscos repassando parcialmente a responsabilidade pelo risco a terceiros, como uma empresa de seguros ou uma empresa de serviços gerenciados? A transferência de riscos está se tornando uma estratégia de segurança cada vez mais importante. A organização pode evitar o risco de segurança transferindo-o para outro grupo, outra equipe, outra pessoa ou para uma organização externa?
- **atenuação**. Você pode atenuar riscos alterando de forma proativa a exposição do ativo ao risco ou alterando a importância do ativo para a organização? Pense em uma estratégia de atenuação de riscos se a EPA for menor que o valor do ativo e se você puder realizar ações proativas. A atenuação é a principal estratégia de gerenciamento de riscos. Você pode fazer tudo para reduzir a

probabilidade de ameaça ou o impacto do risco de segurança no ativo?

Planejamento de contingências. O impacto pode ser reduzido com uma resposta a incidentes planejada? Planos de contingência corretamente criados reduzirão o impacto quando um risco se tornar um problema ou um incidente. Após o incidente de segurança, um disparador poderá ser usado para que o plano de contingência seja executado apropriadamente.

Pesquisa

Grande parte dos riscos de projetos de segurança está relacionada a incertezas que envolvem informações incompletas. Geralmente, os riscos de segurança relacionados à falta de conhecimento podem ser resolvidos ou gerenciados de forma eficaz se for possível aprender mais sobre a ameaça, a exploração, as vulnerabilidades ou sobre o próprio ativo antes de continuar.

Por exemplo, uma equipe pode optar por realizar uma avaliação de vulnerabilidade ou conduzir uma análise de segurança para aprender mais sobre o ambiente ou a habilidade da equipe em reagir a uma violação de segurança antes de concluir o plano de implementação de segurança. Se a decisão da equipe for executar uma pesquisa, o Plano de Ação de Segurança deverá conter uma proposta de pesquisa adequada que inclua as áreas a serem testadas e os problemas a serem respondidos, como a criação da equipe e os equipamentos necessários.

Aceitação

Para alguns riscos de segurança, principalmente ameaças relacionadas a desastres naturais, é simplesmente impraticável intervir com medidas preventivas ou corretivas eficazes. Portanto, a equipe pode simplesmente optar por aceitar a questão de segurança. Contudo, planos de atenuação proativa e contingência reativa ainda devem ser desenvolvidos. Um compromisso corrente em monitorar um risco de segurança deve contar com os recursos apropriados e as medidas de controle estabelecidas.

Observação: a aceitação não é uma estratégia de passividade. O Plano de Ação de Segurança da organização deve incluir uma lógica documentada explicando os motivos que levaram a equipe a optar por aceitar o risco.

Evitar Riscos

Um risco de segurança pode ser identificado como facilmente controlável por meio da alteração do escopo de avaliação. A alteração do escopo de avaliação realizada para "eliminar" totalmente o risco de segurança é chamada de técnica de evitação. Nesses casos, o Plano de Ação de Segurança deve incluir a documentação da lógica para essas decisões e o plano de implementação de segurança deve ser atualizado com os processos de alteração de escopo e com as alterações de design necessárias.

Transferência

Às vezes, é possível transferir um risco de segurança para que seja gerenciado por uma entidade externa à organização. Estes são alguns exemplos de transferência de risco de segurança:

- Seguro.

- Uso de consultores externos mais especializados.

- Serviços terceirizados.

A transferência do risco de segurança não significa que ele será eliminado. Normalmente, uma estratégia de transferência gera novos riscos de segurança que ainda exigem gerenciamento proativo, mas a transferência do risco reduz a ameaça a um nível mais aceitável. Por exemplo, a terceirização da infra-estrutura de TI pode transferir riscos de segurança para fora da equipe de segurança, mas também pode introduzir novos riscos relacionados à confidencialidade dos ativos que a organização está tentando proteger.

atenuação

A atenuação de riscos de segurança envolve a execução de ações proativas que impedirão que um risco de segurança ocorra ou reduzirão o impacto ou as conseqüências a um nível aceitável. O gerenciamento proativo de riscos de segurança por meio de atenuação difere da abordagem de evitação. A atenuação concentra-se na prevenção e na minimização das ameaças a níveis aceitáveis. Já a evitação de riscos de segurança altera o escopo da avaliação para impedir que as atividades que envolvem um risco inaceitável ocorram.

O objetivo principal da atenuação de riscos de segurança é reduzir a probabilidade de ocorrência da ameaça. Por exemplo, a utilização de uma diretiva de senha forte reduzirá a probabilidade de um usuário externo adivinhar uma senha para acessar o sistema da folha de pagamento.

Planejamento de contingências

O planejamento de contingências de risco de segurança envolve a criação de um ou mais planos de resposta a incidentes que possam ser ativados caso os esforços realizados para impedir um ataque falhem. É bom criar planos de contingência para todos os riscos de segurança, inclusive aqueles que têm planos de atenuação. A razão disso é muito simples: mesmo que a organização desenvolva bons planos de segurança proativos, poderá haver ameaças, explorações ou vulnerabilidades desconhecidas capazes de danificar ativos.

O planejamento de contingências de segurança precisa informar o que deverá ser feito se a ameaça ocorrer e precisa concentrar-se na conseqüência e em como minimizar o impacto no ativo. A equipe deve criar planos de resposta a incidentes e planos de restabelecimento de negócios para garantir que você possa reagir de forma eficaz durante e após um ataque.

Você pode estabelecer valores disparadores para planos de contingência com base no tipo de ameaça, exploração ou vulnerabilidade que possa ser encontrado. Por segurança, um disparador é geralmente um evento. Isso significa que é preciso que haja uma maneira de registrar esse evento e de notificar a equipe de resposta adequada para a execução dos planos de contingência.

Existem dois tipos de disparadores de planos de contingência:

- **Disparadores agendados**. Os disparadores agendados são criados de acordo com datas, geralmente a última data em que algo deva ocorrer. As datas podem ser definidas de acordo com diretrizes organizacionais ou legais que proscrevam quando determinadas medidas de segurança ocorrem.
- **Disparadores de limite.** Disparadores de limite dependem de itens que possam ser medidos ou contados. Por exemplo, um evento auditado registrado por um sistema de detecção de intrusão pode garantir um exame e a possível ativação de um plano de contingência.

É importante que a equipe de segurança concorde com outras equipes da organização a respeito de disparadores de planos de contingência e de medidas associadas a eles para que não haja atraso na execução desses planos.

Atividades de agendamento

O agendamento de atividades de gerenciamento e controle de riscos de segurança não difere da abordagem recomendada pela MSF para o agendamento de atividades de projeto em geral. É importante que a equipe de segurança compreenda que as atividades de correção ou controle de segurança são uma parte esperada da avaliação e do gerenciamento de riscos de segurança.

Resultados

O resultado da produção do Plano de Ação de Segurança deve incluir planos de gerenciamento de segurança proativos e reativos que usem uma das seis abordagens apresentadas acima: pesquisa, aceitação, evitação, transferência, atenuação ou o desenvolvimento de planos de contingência. As tarefas específicas para a implementação desses planos de segurança devem ser integradas aos agendamentos padrão de implementação de segurança. Se houver alterações no ambiente técnico, elas deverão ser documentadas em uma especificação funcional.

O agendamento e o Plano de Ação de Segurança devem ser responsáveis por ajustes em recursos e escopos dedicados, o que resultará em um conjunto de itens de ação de segurança que especificam que tarefas individuais devem ser concluídas por membros da equipe de segurança. A lista mestra de riscos de segurança deve ser atualizada para refletir as informações adicionais incluídas nos planos proativos de contingência (atenuação) e reativos. É conveniente resumir os planos de gerenciamento de riscos de segurança em uma única área do documento no formulário de ação de riscos de segurança.

Atualizando o agendamento de implementação de segurança e o plano de implementação de segurança

Os planos de implementação de segurança devem incluir planos proativos e reativos. Ao atualizar o plano de implementação de segurança, considere o seguinte:

- As condições do risco, inclusive a probabilidade de ocorrência e o impacto do risco
A alteração de condições, como a maior probabilidade de um risco ocorrer ou o menor impacto financeiro de um risco, exigirá que a equipe atualize o plano de gerenciamento de riscos.
- A eficácia do esforço de atenuação
A equipe pode achar que alguns dos esforços de atenuação são ineficazes. Freqüentemente, isso ocorre quando uma diretiva técnica que entra em conflito com processos de negócios é implementada. Às vezes, os funcionários subvertem a diretiva técnica encontrando soluções temporárias para ela a fim de atingir seus objetivos de negócios.
- A eficácia de planos de contingência e disparadores
Ao longo do tempo, os riscos de segurança identificados no plano de gerenciamento de riscos ocorrem. Após o incidente de segurança, determine se os planos de contingência e os disparadores de inicialização de respostas foram eficazes.

Sua equipe deve monitorar riscos de segurança nos três intervalos de tempo a seguir:

- **Tempo real**. Use aplicativos, como software de detecção de intrusão, para monitorar continuamente computadores e dispositivos de rede e para tomar decisões predeterminadas com base no risco.
- **Periódico**. Avalie riscos regularmente a períodos agendados, como bimestral ou trimestralmente.
- **Ad hoc**. Avalie riscos a intervalos não agendados. O monitoramento ad hoc quase sempre é realizado em resposta a um incidente de segurança crítico ou a uma alteração na rede.

Desenvolvimento de correção de risco de segurança

O desenvolvimento de contramedidas e procedimentos operacionais são essenciais para a estratégia de segurança da organização. Os riscos de segurança podem ser gerenciados de forma proativa por meio de um processo de proteção

tecnológica ou do desenvolvimento de diretivas que englobem a organização inteira.
Geralmente, a instalação padrão de um sistema operacional, um aplicativo ou um banco de dados tem configurações de segurança pouco severas para simplificar o trabalho do administrador de TI ou do desenvolvedor de software. Antes da implantação de produção dessas tecnologias, a tecnologia que está sendo implantada deve fazer parte de um "processo de proteção".
O processo de proteção do servidor pode envolver a remoção de configurações de segurança padrão e de componentes de software desnecessários. A equipe de TI deve se manter atualizada em relação a vulnerabilidades de tecnologia conhecidas e a explorações atuais para instalar as versões mais recentes de hotfixes de software e segurança.
O processo de desenvolvimento de estratégias de segurança também inclui o desenvolvimento de sistemas, diretivas e procedimentos para controlar e criar relatórios de riscos de segurança não percebidos. Isso ajudará a verificar se as medidas preventivas da infra-estrutura de tecnologia estão funcionando e a validar a eficácia das novas diretivas e procedimentos.
Também deve haver um sistema de relatórios para registrar eventos suspeitos ou ameaças em potencial que exijam atenção imediata. Além de um sistema automatizado para o controle de riscos de segurança, um processo manual também pode ser usado. O controle de riscos de segurança permite que a equipe do projeto faça ajustes a planos para acomodar novos riscos de segurança.
O controle é a função de monitoramento do plano de ação de risco. Isso é essencial para a implementação eficaz de planos de ação de segurança. O controle garante que medidas preventivas ou planos de contingência sejam concluídos de forma adequada e dentro de restrições de recursos do projeto. Durante o controle de risco, as principais atividade executadas pela equipe são o monitoramento de medidas de risco e a certificação de que eventos serão disparados para que ações de risco planejadas entrem em vigor.

Objetivos
O objetivo do processo de desenvolvimento de correções é documentar alterações necessárias de arquitetura, bem como novos processos ou alterações no procedimento.

Informações
As principais informações para o processo de desenvolvimento de correção de risco de segurança são os planos de risco de segurança que contêm a atenuação de segurança específica e os planos de contingência que determinam as ameaças, as explorações e as vulnerabilidades dos riscos de segurança da organização. O desenvolvimento de correções também requer que sistemas e processos sejam desenvolvidos para monitorar os disparadores identificados para os planos de contingência que podem ser executados.

Atividades de desenvolvimento
As atividades de desenvolvimento do processo de correção de risco de segurança são semelhantes às atividades de desenvolvimento de um projeto comum de desenvolvimento de infra-estrutura. Por exemplo, o desenvolvimento de métodos para o gerenciamento de alterações de patches do sistema. Alterações de design realizadas na infra-estrutura devem ser documentadas em uma especificação funcional, e talvez diretivas e procedimentos precisem ser modificados para acomodar os novos requisitos de segurança. Durante esse processo, se novos sistemas forem implementados para fornecer funcionalidade de monitoramento e auditoria, o design e o gerenciamento dos sistemas também deverão ser especificados.
Estes são alguns exemplos de estatísticas de projeto às quais podem ser atribuídas estatísticas de disparadores agendados e que devem ser continuamente controladas:

- Boletins de segurança abertos e não resolvidos de um aplicativo, de um serviço ou de um sistema operacional.
- Média de horas extras registradas por semana pelos engenheiros de infra-estrutura.
- O número de revisões de requisitos ou solicitações de gerenciamento de

alterações por semana.

Procedimentos de criação de relatórios de status de risco também devem ser desenvolvidos nesta fase. A criação de relatórios de risco deve operar em dois níveis: para a própria equipe e para a criação de relatórios externos para o conselho do projeto.

Para a equipe de segurança, relatórios regulares de status de risco devem levar em consideração estas quatro possíveis situações de gerenciamento de riscos que se aplicam a cada risco:

- Um risco é resolvido, concluindo o plano de ação de risco. O risco totalmente resolvido deve ser documentado como fechado e arquivado no Plano de Ação de Segurança.
- Ações de risco são consistentes com o plano de gerenciamento de riscos e estão de acordo com sua agenda.
- Algumas ações de risco não estão de acordo com o plano de gerenciamento de riscos. Nesse caso, medidas corretivas devem ser definidas e implementadas.
- A situação de risco mudou significativamente em relação a um ou mais riscos e, portanto, o plano de ação de risco deve ser reformulado.

Para a criação de relatórios externos para o conselho do projeto e outros participantes, a equipe deve relatar os principais riscos e resumir o status das ações de gerenciamento de riscos. Também é útil mostrar a classificação de riscos anterior e o número de vezes que cada risco esteve na lista dos principais riscos.

À medida que a equipe do projeto executa ações para gerenciar riscos, a exposição total de riscos do projeto deve começar a se aproximar de níveis aceitáveis.

Resultados

O resultado da fase de correção é a especificação das alterações de segurança que devem ser atualizadas nos seguintes itens:

- Especificação funcional

Procedimentos e diretivas operacionais

- Planos de implementação de segurança atualizados
- Agendamentos de implementação de segurança atualizados

↑

Teste de correções de segurança

A etapa de teste de correção de segurança foi criada para garantir que a eficácia dos planos de segurança seja testada. A equipe deve executar atividades relacionadas ao teste das estratégias proativas e reativas (contramedidas e procedimentos) para determinar a eficácia do Plano de Ação de Segurança.

Para medir a eficácia de contramedidas, diretivas e procedimentos recentemente desenvolvidos, você deve examinar cada risco a ser abordado e testar a estratégia associada a esses riscos em relação a ameaças, explorações, vulnerabilidades e ativos da organização.

Talvez seja necessário, com base em testes de correção de risco de segurança, modificar o plano de ação de segurança para melhorar sua eficácia, sua validade e sua capacidade de resposta a eventos disparadores de segurança.

Os resultados e as lições aprendidas com a execução dos planos de teste de segurança são incorporados a um documento de teste para que se tornem parte da base de conhecimento de segurança da organização. É importante coletar o máximo possível de informações durante o teste para determinar a eficácia desses planos.

Objetivos

O objetivo do processo de teste de correção de segurança é testar a eficácia dos diversos planos de segurança que a equipe do projeto criou para os principais riscos de segurança. Os planos de ação de segurança devem avaliar e testar o seguinte:

- A eficácia dos planos de atenuação e contingência.

- As estatísticas de segurança associadas a eventos ou disparadores de planos de contingência.
- Contramedidas de segurança. Podem incluir uma segunda avaliação de vulnerabilidade para determinar se estas foram implementadas corretamente.

Informações
As informações sobre o processo de controle de riscos de segurança são os formulários de ação de segurança que descrevem detalhadamente as atividades a serem realizadas por membros da equipe do projeto para ajudar a abordar cada questão de segurança. Os resultados dos testes devem documentar a eficácia dos planos proativos e reativos para determinar se são apropriados para os requisitos de segurança da organização.

Atividades de teste
As atividades de teste de correção de segurança devem medir a eficácia de cada contramedida e plano de incidente desenvolvido. É importante manter testes contínuos de correção de risco de segurança para detectar os riscos de segurança secundários que possam surgir devido a novas contramedidas.

Resultados
O resultado da etapa de teste de correção de segurança é um documento ou um "banco de dados de questões" que pode ajudar a documentar o andamento, até a conclusão, da implementação dos planos de ação de segurança da organização. É útil que a equipe de teste faça um resumo das estratégias de segurança que funcionaram e das que não funcionaram. Esse resumo também deve informar a eficácia das diretivas e dos procedimentos criados recentemente.

Registrando conhecimento sobre segurança
O conhecimento adquirido durante a avaliação de segurança e o processo de implementação deve ser registrado para uso futuro. Essa é a sexta e última fase do processo de avaliação de risco de segurança. Ela acrescenta uma perspectiva estratégica, empresarial ou organizacional às atividades de gerenciamento de riscos de segurança.

É extremamente importante que as contramedidas, as diretivas e os procedimentos desenvolvidos durante essa avaliação de segurança sejam registrados para que possam ser reutilizados por futuras equipes de projeto. À medida que sua organização inicia futuras iniciativas de TI, esses projetos podem usar o conhecimento adquirido na avaliação para garantir que as novas soluções implementadas sejam seguras.

O aprendizado proveniente da avaliação de risco de segurança deve ser registrado em um formato conveniente para fornecer as informações mais atualizadas. O registro de conhecimentos sobre segurança concentra-se nestes três objetivos principais:

- O registro de lições aprendidas, especialmente aquelas que estão relacionadas à identificação de riscos de segurança e às estratégias de atenuação bem-sucedidas, para o benefício de outras equipes, contribuindo assim com a base de conhecimento de segurança.
- O aumento da eficácia da prontidão operacional no que se refere à capacidade da organização de executar planos de resposta a incidentes e reutilizá-los em outras áreas.
- O aperfeiçoamento do processo de avaliação de risco de segurança, por meio do registro de comentários da equipe.

Registrando o aprendizado dos riscos de segurança

A classificação de riscos de segurança é um método poderoso de garantir que as lições aprendidas em experiências anteriores sejam disponibilizadas a equipes que executarão futuras avaliações de risco de segurança. Estes são três importantes aspectos da aprendizagem que são freqüentemente registrados com as seguintes classificações de risco:

1. **Novos riscos**. Se encontrar um problema que não tenha sido identificado anteriormente como risco de segurança, a equipe deverá rever se algum sinal (ameaças, explorações, vulnerabilidades ou outros indicadores) poderia ter previsto o risco de segurança. É possível que as listas de riscos de segurança existentes precisem ser atualizadas para ajudar na futura identificação da condição do risco de segurança. Também é possível que a equipe tenha

identificado um novo risco de segurança que deva ser adicionado ao knowledge base de segurança existente.

2. **Estratégias de atenuação bem-sucedidas**. Registre a experiência de estratégias bem e malsucedidas para atenuar riscos de segurança. O uso de uma classificação padrão de riscos de segurança oferece uma maneira significativa de agrupar riscos relacionados para que as equipes possam encontrar com facilidade detalhes de estratégias de gerenciamento de riscos de segurança aplicadas com êxito no passado.
3. **Estratégias de contingência bem-sucedidas**. Se um plano de contingência funcionar para proteger um ativo contra um tipo específico de vulnerabilidade, ele poderá ser útil para proteger outro ativo.

Gerenciando o aprendizado dos riscos de segurança

As organizações que usam técnicas de gerenciamento de riscos de segurança freqüentemente descobrem que precisam criar uma abordagem estruturada para o gerenciamento de riscos de segurança. Para facilitar essa tarefa com êxito, estas três condições devem ser atendidas:

1. Compartilhe a responsabilidade com indivíduos da sua equipe de segurança definindo os proprietários de áreas específicas de classificação de riscos de segurança com aprovação para alterações. A decisão de quem será o proprietário está relacionada ao tipo e à classificação do ativo.
2. Procure equilibrar as classificações de riscos de segurança, a necessidade de contramedidas abrangentes, a complexidade e a facilidade de uso. Às vezes, a criação de classificações de riscos diferentes para tipos de projeto diferentes pode melhorar drasticamente a facilidade de uso.
3. Mantenha a uma base de conhecimento de segurança para armazenar classificações, definições e testes de riscos de segurança, critérios de eficácia de monitoramento e medidas para registrar experiências operacionais e de usuários das novas medidas de segurança.

Classificações de riscos de segurança específicas do contexto

A identificação de riscos de segurança pode ser aperfeiçoada com o desenvolvimento de classificações de risco para implementações de soluções

específicas. Por exemplo, em um projeto de desenvolvimento de aplicativo pode haver classificações específicas de riscos de segurança para esse projeto e classificações de riscos de segurança de um projeto de implantação de infra-estrutura. Com a aquisição de mais experiência em relação ao contexto de segurança, os procedimentos e as diretivas de segurança podem se tornar mais específicos e podem ser associados a estratégias de atenuação bem-sucedidas.

Base de conhecimento de segurança

A base de conhecimento de segurança é um mecanismo formal ou informal usado para arquivar lições a fim de auxiliar futuras avaliações de segurança. Sem algum tipo de base de conhecimento, sua organização pode enfrentar dificuldades para adotar uma abordagem proativa para o gerenciamento de segurança.

Se houver um conjunto conhecido de ameaças, explorações e vulnerabilidades registradas na base de conhecimento, será mais fácil desenvolver um plano de atenuação contra elas devido à pesquisa registrada. O knowledge base de segurança é diferente do banco de dados de gerenciamento de riscos de segurança, que é usado para armazenar e controlar itens, planos e status de riscos de segurança individuais.

Desenvolvendo o gerenciamento de conhecimento sobre riscos de segurança

A base de conhecimento de riscos de segurança é o principal mecanismo de aperfeiçoamento contínuo do gerenciamento de riscos de segurança.

A princípio, é provável que as equipes de processos e projetos de segurança da organização não tenham uma base de conhecimento. As equipes precisam começar do zero sempre que empreendem uma avaliação de risco de segurança. Nesse ambiente, a abordagem do gerenciamento de riscos de segurança geralmente é reativa, ocorrendo após uma violação ou um evento que dispare um projeto. Nessa situação, o objetivo é fazer que a organização eleve seu nível de gerenciamento ativo de riscos de segurança.

Posteriormente, a organização pode desenvolver uma base de conhecimento informal de segurança usando o aprendizado implícito adquirido de membros mais experientes que estão familiarizados com as questões de segurança

relacionadas a pessoas, processos e tecnologias ou de membros que são especialistas no assunto. Geralmente, isso é conseguido com a implementação de um grupo de discussão de segurança. Essa abordagem encoraja o gerenciamento ativo de avaliação de risco de segurança e pode levar a um gerenciamento proativo por meio da introdução de diretivas de segurança.

O primeiro nível de desenvolvimento da base de conhecimento é atingido com o fornecimento de uma abordagem mais estruturada para a identificação de riscos de segurança. Com a indexação e o registro formal de questões de segurança, a organização será capaz de realizar um gerenciamento muito mais proativo à medida que as causas subjacentes dos riscos de segurança começarem a ser identificadas.

Por fim, as organizações maduras registram não somente indicadores que possivelmente levarão a riscos de segurança, mas também as estratégias adotadas para gerenciar esses riscos de segurança e suas taxas de êxito. Com esse tipo de base de conhecimento, a identificação de segurança e as etapas de planejamento do processo de riscos de segurança podem ser baseados na experiência compartilhada de muitas equipes e sua organização pode começar a otimizar os custos do gerenciamento de riscos de segurança.

Ao considerar o modo como a base de conhecimento de riscos de segurança deve ser implementado na organização, lembre-se que a experiência mostra que:

- O valor da base de conhecimento de riscos de segurança aumenta à medida que uma maior parte do trabalho torna-se repetitiva (como a concentração em outros projetos que afetam processos operacionais contínuos ou de segurança).
- Quando a organização está executando uma revisão de segurança semelhante, é mais fácil manter uma base de conhecimento menos complexa.
- O gerenciamento de riscos de segurança não deve se tornar um processo automatizado que impeça a equipe de pensar sobre os riscos de segurança. Mesmo em situações repetitivas, o ambiente de negócios, a habilidade dos atacantes e a tecnologia estão sempre mudando. A equipe de segurança deve avaliar as estratégias adequadas de gerenciamento de riscos de segurança para o ambiente com base nas pessoas, nos processos e nas tecnologias existentes.

Conclusão

Este módulo explica a práticas comprovadas derivadas de métodos de análise de segurança e processos formulados na MSF e na MOF. Ele detalhou os processos usados na SRMD para determinar os custos necessários para proteger os ativos da organização. Por fim, mostrou as etapas recomendadas para a formação de uma equipe de segurança para criar e executar planos de ação de segurança que impedirão ataques contra o ambiente da organização e permitirão que haja uma reação contra esses ataques.

Referências

Para obter informações sobre a MSF, consulte: http://www.microsoft.com/technet/itsolutions/techguide/msf/default.mspx.

Para obter informações sobre a MOF, consulte: http://www.microsoft.com/technet/itsolutions/techguide/mof/default.mspx.

Para obter informações sobre crimes de informática, consulte: http://www.gocsi.com/press/20020407.html.

Para obter informações sobre avaliação de ameaças, consulte: "Threat Assessment of Malicious Code and Human Threats", de Lawrence E. Bassham & W. Timothy Polk: National Institute of Standards and Technology Computer Security Division, em: http://csrc.nist.gov/publications/nistir/threats/index.html.

Para obter informações recomendações de segurança de informações, consulte: http://www.iso-17799.com/.

Para obter informações sobre hackers, consulte: http://www.hackingexposed.com/.

Para obter informações sobre ameaças à segurança na Microsoft TechNet, consulte: http://www.microsoft.com/technet/security/bestprac/bpent/sec1/secthret.mspx.

Para obter informações sobre atribuição de valores de ativos do National Institute of Standards and Technology, consulte: http://csrc.nist.gov/asset/